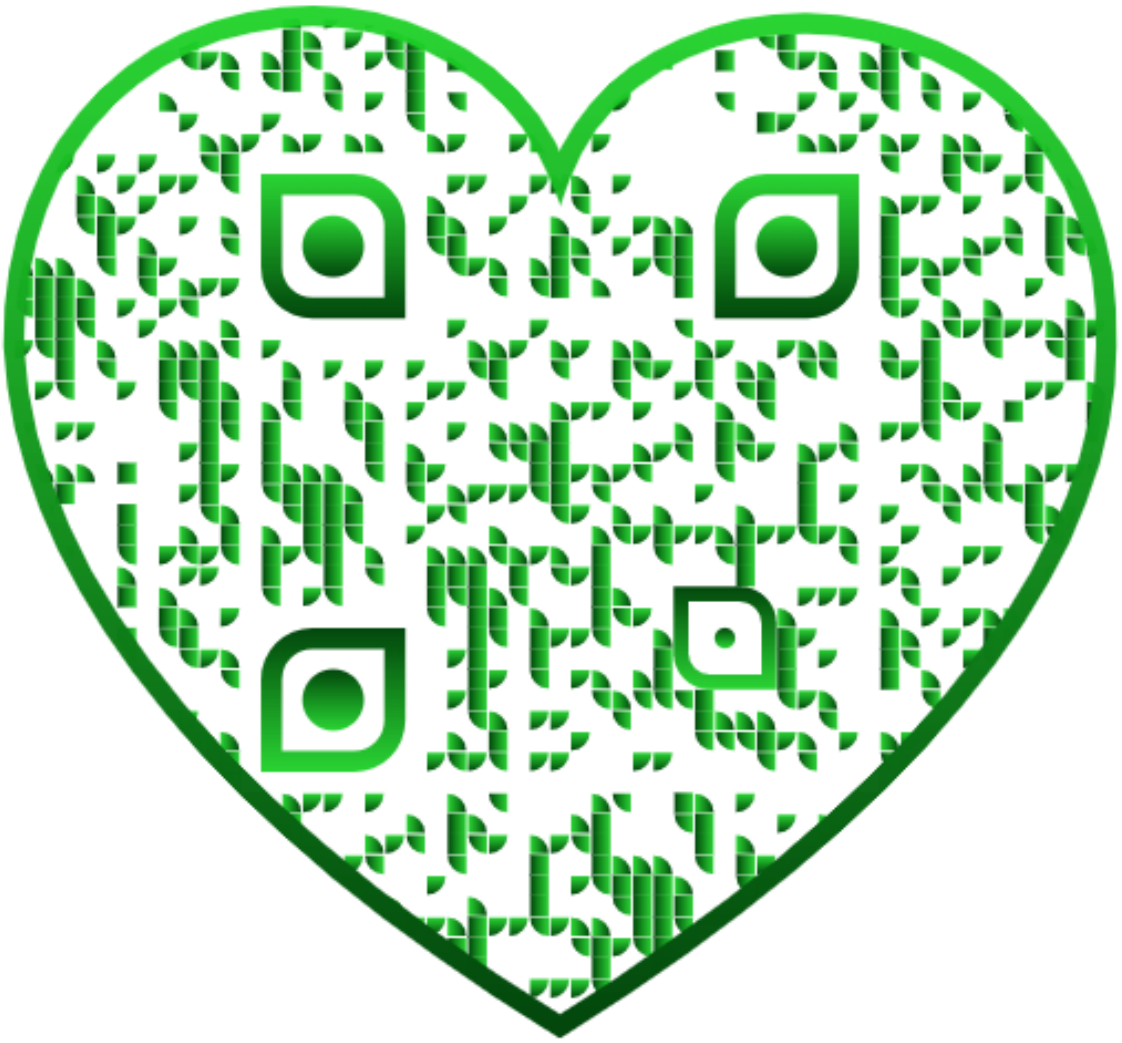
Hervé Lehning

LA BIBLE DES CODES SE~CRETS

Flammarion



Hervé Lehning

LA BIBLE DES CODES SECRETS

Flammarion

Hervé Lehning

La Bible des codes secrets Flammarion

Ce livre a été établi en collaboration avec Xavier Müller.

© Flammarion, 2019

ISBN Epub : 9782081492370
ISBN PDF Web : 9782081492394
Le livre a été imprimé sous les références : ISBN : 9782081490017

Ouvrage composé et converti par Pixellence (59100 Roubaix)

Présentation de l'éditeur

Toutes les clés pour y voir clair
Ils sont partout : dans votre carte bleue, votre téléphone portable ou votre box Internet. Ils ont déclenché des guerres, fait gagner des batailles et mis des États en difficulté – souvenez-vous de l'affaire Snowden…
Ce sont les codes secrets, un procédé vieux comme Homère, qui les utilisait déjà, et cher à César, aux Templiers comme à Henri IV qui en abusait dans sa correspondance amoureuse.
Zigzag, code pourpre, cadran d'Alberti, chiffre de Bazeries, machine de Gripenstierna, Enigma, masque jetable, Vernam, algorithme RSA, etc. : voici enfin l'ouvrage qui manquait pour percer tous leurs mystères. Il est enrichi de nombreux exemples pratiques, qui proposent autant de pistes pour chiffrer à votre tour !
Cpoof mfduvsf.

Normalien et agrégé de mathématiques, Hervé Lehning est fou de cryptographie. Membre de l'Association des réservistes du chiffre et de la sécurité de l'information, il a notamment expertisé la boîte à chiffrer d'Henri II. Son précédent livre, *Toutes les mathématiques du monde*, est devenu un classique traduit en plusieurs langues.

La Bible des codes secrets

PRÉFACE

Avertissement : vous tenez entre les mains un document rare ! Les livres sur les codes secrets se comptent par centaines. Mais aucun ne ressemble à celui-là. En publiant *La Bible des codes secrets*, nous avons voulu proposer aux lecteurs un ouvrage de référence qui remplit un double rôle. Le premier est de vous faire voyager à travers le monde mystérieux et intrigant (et des intrigues, il y en aura !) des secrets de l'Histoire, du manuscrit de Voynich du XVe siècle – à la langue elfique jamais décryptée – jusqu'à Radio Londres et ses célèbres messages codés de l'émission « Les Français parlent aux Français ».

Le monde dans lequel vous vous apprêtez à entrer est longtemps resté l'apanage des puissants. Il a été dissimulé sciemment à l'homme de la rue. Des décennies durant, les historiens se sont heurtés au silence des autorités afin d'obtenir la vérité sur le chiffrement des transmissions de la Première et de la Seconde Guerre mondiale, notamment. Lors de la Révolution, Marie-Antoinette entretenait sa liaison secrète avec le comte Axel de Fersen en lui écrivant des lettres d'amour chiffrées avec l'un des meilleurs codes de l'époque, même si toutefois elle l'utilisait mal.

Aujourd'hui, les spécialistes ont levé le voile sur ces secrets anciens, mais l'intégralité des connaissances en la matière n'a pas été mise à la disposition du grand public, en tout cas sous la forme d'une somme riche et informative

qui, à la manière des pyramides qui contemplaient quarante siècles d'histoire, couvre toutes les époques. Saviez-vous par exemple que, lorsqu'il a tenté d'exporter la révolution cubaine en Bolivie, Che Guevara communiquait avec Fidel Castro avec le même code que celui utilisé pour le téléphone rouge entre Américains et Russes ? Savoureux, n'est-ce pas ? Ou que les arcanes de la célèbre Enigma, la machine de chiffrement, furent en partie percés grâce à la trahison d'un fonctionnaire allemand du bureau du Chiffre ?

Madame, demain cinq heures au square

Le premier objectif de cet ouvrage, largement enrichi depuis sa première édition en 2012 (*L'Univers des codes secrets*, Ixelles), est ainsi historique. Le chiffre – l'art de chiffrer des messages – a d'abord été diplomatique et militaire, avant de servir le secret des affaires dès le XIX^{e} siècle et aussi un champ plus anecdotique des relations humaines… les correspondances amoureuses. Son inverse, le décryptement, a mené à une sophistication des techniques de chiffrement et donc à une lutte incessante entre chiffreurs et décrypteurs.

Le second but du livre est de vous donner les clefs (dans les deux sens du terme) pour comprendre le fonctionnement véritable des codes secrets. En voici deux exemples :

Fhwwh suhplhuh skudvh hvw fkliiuhh sdu xq vlpsoh ghfdodjh.
Retpyrced a eliciffid sulp erte tuep esarhp ednoces ettec.

Ces deux phrases sont chiffrées. Pour ceux qui ignorent tout de la cryptographie, elles sont sans doute incompréhensibles. Elles représentent pourtant dans leurs formes les plus simples les deux grandes méthodes classiques de chiffrement : la substitution et la transposition. Quand vous aurez lu ce livre, décrypter ces

phrases vous semblera aussi évident que respirer (si, si, je vous le garantis).

Ce livre contient donc parfois des parties un brin techniques (en fait, surtout dans sa seconde moitié). Toutefois, ces parties peuvent cependant être survolées sans dommage pour la compréhension générale. Elles existent pour ceux qui veulent creuser la question. Il en est de même des exercices ludiques marqués CQFD (ce qu'il fallait décrypter). Les plus motivés d'entre vous que rien n'effraie, pas même les pages casse-têtes mathématiques des suppléments d'été des magazines, trouveront là de quoi s'échauffer les neurones.

Erreurs éternelles

Ce double souci, historique et technique, constitue à mon sens l'originalité de cet ouvrage sur les codes secrets. Il ne se contente pas de donner l'importance stratégique des exploits des décrypteurs comme Antoine Rossignol à l'âge classique, Georges Painvin pendant la Première Guerre mondiale ou Alan Turing lors de la Seconde, il essaye aussi de montrer le degré d'ingéniosité qu'ils ont développé, et comment ils ont su exploiter les erreurs de leurs adversaires, erreurs qui ont jalonné toutes les époques. Les méthodes changent, les erreurs restent.

J'ai privilégié un plan structuré à la fois autour des méthodes de chiffrement et de l'Histoire. Tout d'abord, je montrerai à travers des exemples historiques la nécessité de cacher et l'intérêt de décrypter les transmissions. Ensuite, nous verrons le grand principe de la cryptographie moderne, proposé à la fin du XIX^{e} siècle par Auguste Kerckhoffs, selon lequel un système cryptographique ne doit pas reposer sur le secret des méthodes, des algorithmes comme on le formulerait aujourd'hui, mais sur celui d'une clef qu'on change périodiquement. De tels chiffres

existaient déjà depuis la Renaissance, ce sont les chiffres par substitution poly-alphabétique, dont le plus connu est attribué à Blaise de Vigenère, mais ils furent peu usités avant le XIXe siècle, du fait de la difficulté de les mettre en œuvre à la main. De ce fait, on leur préféra à l'époque les chiffres par substitution mono-alphabétiques. J'illustrerai à quel point ils sont faciles à casser, que ce soit sur des exemples inventés pour l'occasion ou sur des exemples de chiffres réels.

Deux par deux

Une amélioration arriva au XIXe siècle avec l'idée de substituer les lettres deux par deux et non plus individuellement. L'idée fut poussée au XXe siècle avec les trigrammes (trois par trois) puis les polygrammes, ce qui marqua la première incursion des mathématiques en tant que telles en cryptographie. Je poursuivrai en revenant aux XVIIe et XVIIIe siècles et la révolution cryptographique initiée par Antoine Rossignol, qui eut l'idée de chiffrer les syllabes, comme les lettres ou les mots par des nombres, concevant ainsi les premiers dictionnaires chiffrés. Bien employés, ces dictionnaires pouvaient résister aux décrypteurs, mais ils ont aussi conduit au désastre d'une armée napoléonienne peu avisée en termes de codes secrets…

Les préludes de la Première Guerre mondiale virent le développement de systèmes par transposition, dans lesquels on chiffre un message en fabriquant une anagramme. Combinés avec des substitutions poly-alphabétiques, ces systèmes cryptographiques furent les meilleurs de la Première Guerre mondiale. Cependant, les messages étaient longs à chiffrer, comme à déchiffrer et mal adaptés à une guerre de mouvement, ce qui a poussé au développement de machines à chiffrer dont l'Enigma de l'armée allemande. Elle produisait un chiffre poly-alphabétique qu'on croyait indécryptable et qui fut pourtant cassé par les Polonais d'abord et les Britanniques ensuite. L'utilisation des machines à chiffrer se prolongea après la Seconde Guerre mondiale, mais elles furent ensuite remplacées par des ordinateurs. Des méthodes plus mathématiques où, d'une façon étrange, savoir chiffrer ne suffit pas pour savoir déchiffrer, virent alors le jour. Même si ces techniques sont sûres, elles sont menacées aujourd'hui par l'avènement d'un nouveau type de machine :

l'ordinateur quantique. Aujourd'hui encore, la lutte millénaire entre chiffreurs et décrypteurs continue…

1 L’arme de la guerre secrète

Il y a l’histoire avec un grand « H » et il y a *les* histoires. Celles qui échouent dans les notes de bas de page des manuels. Ce sont pourtant souvent celles qui enflamment l’imagination des scénaristes et des romanciers. De César défiant les Germains avec ses messages chiffrés à Radio Londres et l’émission « Les Français parlent aux Français », la guerre vue par le prisme des codes secrets fourmille d’épisodes de ce type, parfois anecdotiques, parfois renversants (y compris sur l’issue de la bataille !). Feuilleter les pages de cette épopée, c’est parcourir dans le désordre deux mille ans d’une « contre-histoire » de notre civilisation, tout aussi palpitante et utile à connaître que la « contre-histoire » de la philosophie que certains ont mis en lumière.

Un exemple de ces coulisses de l’Histoire ? Lombardie, 23 décembre 1796. Voilà dix mois que l’armée d’Italie de Bonaparte tient le siège de la ville de Mantoue, où s’est recluse l’armée autrichienne. Une armée (également autrichienne) de secours a bien tenté de percer les lignes françaises pour venir à son secours, mais elle a subi un grave revers lors de la célèbre bataille du pont d’Arcole, en novembre. En cette veille de Noël, des sentinelles veillant aux abords de Mantoue arrêtent un quidam cherchant à pénétrer dans la cité occupée. Malgré l’absence de preuve, ils la soupçonnent de complicité avec les Autrichiens et le conduisent au général Dumas, le père du futur Alexandre

Dumas qui racontera l'anecdote dans ses mémoires. Le pauvre hère cacherait-il un espion ? Le général pense alors à une méthode antique décrite par César dans *La Guerre des Gaules*, mais qui avait déjà cours en Extrême-Orient longtemps auparavant. Les seigneurs chinois écrivaient leurs messages sur de la soie très fine, qu'ils enrobaient ensuite de cire. Le messager n'avait plus qu'à avaler la boulette pour être sûr que le message ne soit pas intercepté.

Dumas fait donc servir un purgatif au prisonnier, qui accouche… peu après d'un message enfermé dans une boulette de cire ! Ecrit de la main du général autrichien Alvintzy, le texte annonce l'arrivée de renforts :

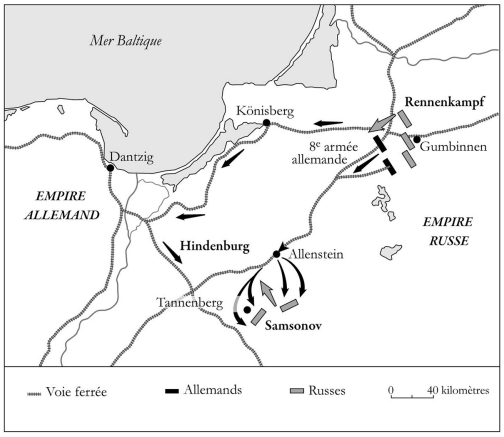
> Selon toute probabilité, le mouvement que je ferai aura lieu le 13 ou 14 janvier ; je déboucherai avec trente mille hommes par le plateau de Rivoli, et j'expédierai Provera avec dix mille hommes par l'Adige sur Legnago, avec un convoi considérable. Quand vous entendrez le canon, faites une sortie pour faciliter son mouvement.

Le procédé était habile et les Français, chanceux d'intercepter le message. Bonaparte envoya des éclaireurs dans le nord de l'Italie qui confirmèrent que l'armée d'Alvintzy s'était effectivement divisée en deux corps ne devant se réunir qu'à Rivoli. Les Français se battaient à un contre deux dans le conflit. Grâce à ce renseignement volé, les soldats de Napoléon compensèrent leur infériorité numérique. Ils affrontèrent séparément les deux armées et réussirent à bouter, courant 1797, les Autrichiens hors de la péninsule italienne. Quand un laxatif sauve la mise du porteur de bicorne…

Lire dans le jeu de ses adversaires

Pourquoi le général autrichien Alvintzy n'avait-il pas chiffré son message ? L'histoire retient difficilement les leçons du passé… Un siècle plus tard, les Russes commirent

la même erreur et subirent une déroute à la hauteur de cet impardonnable oubli. Quand la Première Guerre mondiale éclata, le 4 août 1914, la Russie n'était pas prête à lancer son énorme armée de plus de 5 millions d'hommes sur l'Allemagne. C'est pourquoi celle-ci tenta de profiter du délai accordé pour annihiler les armées françaises dans un vaste plan d'encerclement en six semaines. L'Allemagne n'avait laissé en Prusse orientale qu'une armée de 200 000 hommes. À la surprise des Allemands, les Russes attaquèrent le 17 août avec deux armées de 400 000 hommes chacune. Le plan russe était simple : prendre l'ennemi en tenaille. Pendant que la première armée russe, commandée par Pavel Rennenkampf, attaquait à l'est, la seconde, sous les ordres d'Alexandre Samsonov, contournerait les lignes allemandes par le sud, pour les prendre à revers.



Lors de l'invasion de la Prusse orientale en août 1914, les Russes cherchaient à défaire l'armée allemande en l'encerclant. Leur plan fut anéanti par l'absence de transmissions chiffrées, qui conduisit au désastre de Tannenberg.

Sur le papier la victoire était assurée, à un détail près : les communications. Incapables d'équiper les distances parcourues en lignes télégraphiques, les Russes utilisaient la radio… que les Allemands écoutaient bien sûr. Or aucun

de ces précieux livres de codes nécessaires au chiffrement des messages n'ayant été livré à temps, les transmissions se faisaient en clair. Autrement dit, les Allemands étaient invités aux réunions d'état-major des Russes ! Malgré cet avantage, l'invasion de la Prusse orientale commença sous de bons auspices : les Allemands furent contraints de prélever du front ouest deux corps d'armée, ce qui allégea d'autant la pression sur l'armée française. Pour éviter l'encerclement, le général en chef allemand ordonna la retraite sur la Vistule, abandonnant ainsi la totalité de la Prusse orientale. Il fut aussitôt démis de ses fonctions et remplacé par Paul von Hindenburg assisté d'Erich Ludendorff, qui reprirent l'offensive.

Troupes russes en route vers le front en 1916. Ce que l'on a appelé à l'époque le « rouleau compresseur » se montra mal préparé et incapable de lutter sérieusement contre l'Allemagne, d'autant que son chiffre était faible.

Ce changement aux manettes marqua un tournant dans la bataille. Quand Hindenburg et Ludendorff apprirent grâce aux messages ennemis captés que leur homologue russe Rennenkampf avait réduit son allure, craignant que les Allemands n'échappent à la manœuvre, ils laissèrent un mince cordon de cavalerie devant celui-ci et utilisèrent l'excellent réseau ferré allemand pour porter tout leur effort sur Samsonov, leur second poursuivant, dont ils connaissaient la localisation exacte. La bataille de

Tannenberg qui s'ensuivit fut la seule victoire décisive de la Première Guerre mondiale. La seconde armée russe fut anéantie et Samsonov se suicida pour échapper à la capture et à la honte. Les Russes retinrent la douloureuse leçon : ils se mirent à chiffrer systématiquement leurs messages, mais avec un savoir-faire approximatif. Si bien que, jusqu'à la fin de la guerre, ils livrèrent combat sans se douter que l'adversaire continuait à lire leurs plans par-dessus leurs épaules !

Le miracle de la Vistule

Les déboires de la Russie ne s'arrêtèrent pas là. Immédiatement après la Grande Guerre, ils payèrent à nouveau le prix de leur manque de savoir-faire en matière de chiffrement. Le théâtre du conflit fut cette fois la Vistule, le principal fleuve de Pologne. En 1920, la Russie devenue soviétique se lança dans la reconquête du pays, devenu indépendant depuis le traité de Versailles. Lénine, au pouvoir à Moscou, rêvait aussi d'exporter la révolution en Europe occidentale et la Pologne constituait un verrou contre ce projet.

Plus puissante, l'armée russe semblait devoir l'emporter, mais son adversaire détenait une botte secrète : le service chargé du décryptement des transmissions, le *bureau du Chiffre*, où officiaient des mathématiciens de haut niveau comme Waclaw Sierpiński (1882-1969) (plus connu du grand public pour des fractales portant son nom) et Stefan Mazurkiewicz (1888-1945), deux grands noms de l'analyse mathématique (la branche des mathématiques qui s'intéresse aux fonctions).

Ce bureau du Chiffre décrypta les dépêches russes et révéla dans le dispositif soviétique une faiblesse qui conduisit l'armée polonaise à la victoire. Le clergé polonais, qui avait demandé à la population de prier pour le salut du

pays, qualifia ce triomphe de « miracle de la Vistule », du nom du lieu où se situa la bataille clef. Le décryptement des communications russes : voilà le seul vrai miracle qui avait eu lieu.

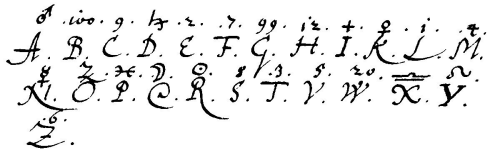
Le message était de la poudre aux yeux

Historiquement, le « miracle de la Vistule » n'était pas la première victoire à mettre au crédit des décrypteurs. Pour ne citer qu'un exemple tiré du Grand Livre de la France, déjà en 1626 Henri II de Bourbon avait su bénéficier des compétences du bureau du Chiffre. Voici les détails de la situation. Le prince de Condé, catholique, tenait depuis un moment le siège de Réalmont, une place forte protestante située dans le département du Tarn. L'adversaire lui résistant vaillamment, notamment grâce à ses canons, il s'apprêtait à prendre ses cliques et ses claques lorsque ses troupes interceptèrent un homme sortant de la ville. Cela vous rappelle l'histoire lombarde que nous avons déjà vue ? Oui, à la différence près que l'homme portait sur lui le message, bel et bien chiffré cette fois. Mais que signifiait donc ce charabia formé de lettres et de symboles ?

Antoine Rossignol (1600-1682). Selon une légende, grâce à sa capacité à percer les messages codés, le mathématicien aurait donné son nom à l'instrument qui permet d'ouvrir les portes sans clef, vu dans de nombreux films. C'est faux, le terme étant attesté quelque deux cents ans avant la naissance de Rossignol.

Pour décoder le message, on fit venir Antoine Rossignol, un jeune mathématicien connu dans la région pour son talent de décrypteur. Qui parvint à faire parler le galimatias… Que disait-il ? Que la ville manquait de poudre et qu'à défaut d'en recevoir, elle serait obligée de se rendre. Les destinataires de la missive étaient les huguenots de Montauban. Habile, Condé renvoya le message décrypté à Réalmont, qui se rendit. À lui seul Rossignol venait d'influer sur le cours de l'Histoire ! Il réitéra son exploit au siège de La Rochelle l'année suivante, si bien que le cardinal de Richelieu le prit à son service. Cet excellent cryptanalyste (un spécialiste du décryptement) modifia ensuite profondément la cryptographie de son époque (voir le chapitre 5).

L'histoire n'a pas retenu la nature du chiffrement du message sortant de la forteresse. Il est cependant probable qu'il utilisait un alphabet chiffré comme le suivant, daté de la même époque (1627) et provenant des archives de la ville de Strasbourg.



Alphabet chiffré utilisé en 1627 par un délégué de Strasbourg. De façon classique, I et J d'une part, U et V d'autre part sont confondus. Quant à V et W, le fait que les deux lettres soient distinctes laisse penser que cet alphabet servait plutôt à chiffrer des textes rédigés en allemand.

Pour exploiter cet alphabet, on remplace chaque lettre par le symbole situé au-dessus. Quelques remarques sur la qualité de ce codage. Il est faible, car si le texte est suffisamment long, il suffit d'isoler le symbole le plus fréquent pour savoir qu'il correspond à la lettre E (la lettre la plus courante en français). Les répétitions à l'intérieur d'un même terme sont également susceptibles de servir à percer le message : des mots comportant des redoublements de lettres comme *munitions*, qui comptent deux N et deux I, ont des structures particulières qui permettent de les chercher sous la forme « ..*+.+.* » où chaque point correspond à un symbole quelconque.

L'aptitude à reconnaître des structures, même en dehors de mathématiques avancées, fait partie des capacités requises en mathématiques comme en cryptologie (la science du chiffrement). Cela explique sans doute que, dès le XVIIe siècle, les grands cryptologues venaient souvent des mathématiques. Dans ce domaine, on trouve François Viète (1540-1603) qui mit sa science au service d'Henri IV, même s'il est davantage connu de nos jours pour ses travaux en

algèbre. Sa démarche était proprement mathématique, car systématique. En particulier, il avait établi une règle, qu'il disait infaillible, selon laquelle dans trois lettres successives, une au moins était une voyelle. Même si ce n'est pas tout à fait exact en français comme le montrent les mots contenant la suite « ntr » en particulier, il s'agit d'une aide précieuse pour localiser les voyelles à coup sûr ou presque.

Les dons de Viète faillirent l'envoyer au bûcher. Parmi toutes les lettres qu'il réussit à décrypter figuraient celles du roi d'Espagne Philippe II. Celui-ci finit par se savoir espionné et, pensant nuire aux Français, avertit le pape qu'Henri IV ne pouvait avoir lu ses dépêches qu'au moyen de la magie noire… L'information dut faire sourire le pape : son propre cryptologue avait cassé quelques chiffres de Philippe II trente ans plus tôt. C'est ainsi que Viète échappa à un éventuel procès en sorcellerie.

Vengeance de cœur

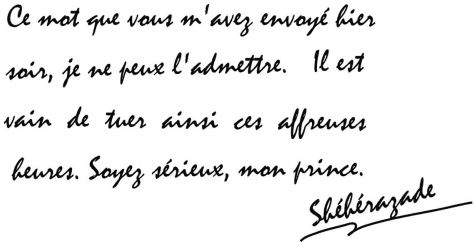
Il existe un autre théâtre de guerre où l'encre des messages chiffrés peut se révéler vénéneuse : la joute amoureuse. La plus vieille histoire mêlant jeux d'amour et de chiffres nous vient d'Homère. La femme de Proétos, le roi de Tirynthe, ayant été éconduite par Bellérophon, « à qui les dieux donnèrent beauté et vigueur », décida de se venger de lui en l'accusant d'être son prétendant devant son mari :

> – Meurs, Proétos, ou tue Bellérophon qui, par violence, a voulu s'unir à moi.
> À ces paroles, la colère saisit le roi. Et il ne tua point Bellérophon, redoutant pieusement ce meurtre dans son esprit ; mais il l'envoya en Lykiè avec des tablettes où il avait tracé des signes de mort, afin qu'il les remît au roi, son beau-père, et que celui-ci le tuât.

Les événements prirent en réalité une autre tournure. Quand le roi de Lykié reçut les fameuses tablettes avec des *signes de mort*, visiblement un message codé, plutôt que de tuer Bellérophon sur-le-champ, il préféra l'envoyer

combattre des monstres, épopée dont il ressortit vivant. Mais le véritable usage des codes secrets en amour, c'est bien sûr pour tenir secret le contenu d'échanges épistolaires. « Il y a des particularités que je ne puis écrire pour avoir perdu le chiffre que j'avais avec vous », regrettait Henri IV dans une lettre à sa maîtresse, la comtesse de Gramont. La pratique semble aussi vieille que l'amour lui-même. Dans l'Inde antique, l'écriture secrète était ainsi l'un des 64 arts que devait posséder la parfaite concubine selon le *Kâmasûtra*.

Masquer la teneur de ses messages, c'est bien. Dissimuler l'acte même d'écrire, c'est encore mieux. Cela évite d'éveiller les soupçons. Je vous propose p. suivante un message que Shéhérazade aurait pu écrire à un amant.


Ce mot que vous m'avez envoyé hier
soir, je ne peux l'admettre. Il est
vain de tuer ainsi ces affreuses
heures. Soyez sérieux, mon prince.
Shéhérazade

Lettre d'une princesse à son amant.

En apparence, rien de compromettant. Pourtant, ces quatre lignes comportent le même message que la phrase suspecte « GI WSMV ZMRKX LIYVIW », à savoir « Ce soir, vingt heures. »

Les deux techniques employées ici pour chiffrer le message s'appellent stéganographie et cryptographie. La première cache le message dans un décorum, tandis que la seconde le code. Notre princesse avait raison de recourir à la stéganographie. À la fin du XIXe siècle, les amants étaient plus enclins à jouer les apprentis cryptologues via les petites annonces des journaux. Un message tel que « GI

WSMV ZMRKX LIYVIW », au milieu de ventes de bois de chauffage ou de recherches de logement, est totalement innocent. De nos jours, les SMS autorisent plus de liberté, nous reviendrons sur la question.

Aussi étonnant que cela puisse paraître, les billets doux échangés par les amoureux, en version chiffrée, eurent leur importance dans l'histoire de la cryptographie. Étienne Bazeries, l'une des grandes figures de la fin du XIXe siècle et du début du XXe, s'amusait à lire les messages personnels chiffrés qui, à l'époque, servaient de moyen de communication à des couples illégitimes. Au mess des officiers de sa garnison, il régalait ses collègues d'histoires scabreuses qu'il lisait sans peine… jusqu'au jour où il annonça qu'il pouvait également lire les messages chiffrés de l'armée sans en connaître le code. Son général prit cette remarque au sérieux et lui demanda de décrypter quelques dépêches du ministère, ce que Bazeries fit sans peine ! Il devint plus tard l'un des éminents cryptologues de l'armée française, puis du ministère des Affaires étrangères.

Étienne Bazeries (1846-1931), l'un des plus fameux cryptologues de son temps.

À un cheveu de la défaite

Si Shéhérazade ensorcelait peut-être les hommes avec ses contes des mille et une nuits, l'exemple que nous avons donné plus haut de stéganographie commençant par « Ce mot que vous m'avez envoyé » aurait peu de chances de nous prendre par surprise aujourd'hui, tant le stratagème paraît grossier. Un autre exemple de stéganographie ? La plus vieille illustration qu'on connaisse de la technique remonte au v^{e} siècle avant notre ère et nous est rapportée par l'historien grec Hérodote. Rappelons que la cryptographie est l'art de cacher le sens d'un message, dont la présence reste évidente. Par exemple, il est manifeste que « FHFL HVW XQ PHVVDJH FRGH » est un message chiffré. Au contraire, la stéganographie consiste à dissimuler l'existence même du message.

Que raconte Hérodote ? Aristagoras, le tyran (l'équivalent d'un despote à l'époque) de la ville de Milet, avait un oncle qui s'appelait Histiée. Alors que ce dernier se trouvait à la cour de Perse comme conseiller, il voulut informer son gendre que le moment était venu de se révolter justement contre la Perse. Pour transmettre ce message, Histiée choisit un esclave dévoué, lui rasa la tête, et écrivit sur son cuir chevelu. Il attendit que les cheveux repoussent et l'envoya à Aristagoras. Une fois parvenu à Milet, l'esclave n'eut plus qu'à se tondre pour délivrer son message. Un peu long, mais efficace comme technique stéganographique.

Dans ses œuvres, Hérodote décrit une autre méthode assez proche, mise à profit cette fois par un certain Démarate, en exil à la cour de Perse. Pour avertir le roi de Sparte d'une attaque imminente, Démarate prit des tablettes de cire avec lesquelles on avait coutume d'écrire, en racla la surface, grava le message secret directement sur leur bois, puis leur rendit leur apparence originelle. Apparemment vierges, elles n'attirèrent pas l'attention en chemin. À leur arrivée à Sparte, la reine Gorgô, une femme d'une grande intelligence, fut frappée d'étonnement face à ces tablettes intactes et eut l'idée de gratter la cire. Elle découvrit ainsi le message de Démarate. Le premier décrypteur de l'Histoire fut donc une femme. Son discernement sauva le monde grec du péril perse (mais causa la mort de son mari, Léonidas, lors de la fameuse bataille des Thermopyles).

Encre sympathique allemande

Un siècle après Hérodote, ce fut au tour d'un militaire grec de révéler certaines de ses méthodes secrètes de stéganographie. Ce chef de guerre était le bien nommé Énée le tacticien. Dans son livre sur l'art du siège, il raconte comment déguiser un message à l'intérieur d'un livre en

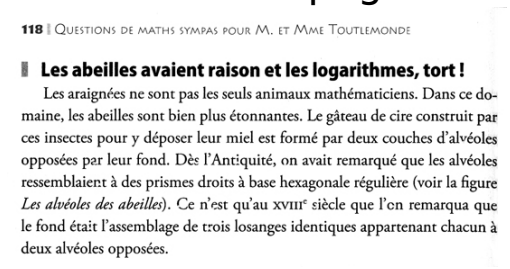
marquant certaines lettres de façon imperceptible, au moyen d'une épingle par exemple. Le message apparaît en recopiant dans l'ordre les lettres ainsi choisies. Cette astuce était encore utilisée par des espions allemands au cours de la Seconde Guerre mondiale pour transmettre leurs renseignements à leur hiérarchie. De l'encre sympathique repérait les lettres. Tous les moyens sont bons, à dire vrai, du moment que le message est déchiffrable par son destinataire et n'éveille aucun soupçon chez les autres, ce qui n'est pas acquis…

Essayez par vous-même : pour cela, prenez un livre et procurez-vous de l'encre sympathique, qui ne devient visible qu'après un léger chauffage. Lait, jus de citron, ou même urine (!) feront l'affaire. À l'aide d'un coton-tige, biffez ensuite les caractères pour former votre message. Laissez sécher et absorbez le surplus avec du buvard : vous n'avez alors plus qu'à transmettre votre livre à son destinataire. Une version modernisée de la même méthode consisterait à passer par des sites anodins sur Internet, tels ceux de ventes aux enchères, pour transmettre vos messages en désignant les lettres par des espaces doubles ou triples entre les mots, par exemple.

À l'inverse, faute d'encre sympathique, vous pouvez tout aussi bien vous contenter d'ajouter des pattes de mouche sous certains caractères du livre. Ainsi, la phrase de Marcel Proust : « Longtemps, je me suis couché de bonne heure. Parfois, à peine ma bougie éteinte, mes yeux se fermaient si vite que je n'avais pas le temps de me dire : Je m'endors. » véhicule le message « lundi », qui peut constituer la réponse à une question.

Ce Qu'il Faut Décrypter Un message dissimulé dans un livre

Un livre a été retrouvé dans la cellule d'un prisonnier. Voici l'une des pages :



118 | Questions de maths sympas pour M. et Mme Toutlemonde

Les abeilles avaient raison et les logarithmes, tort !

Les araignées ne sont pas les seuls animaux mathématiciens. Dans ce domaine, les abeilles sont bien plus étonnantes. Le gâteau de cire construit par ces insectes pour y déposer leur miel est formé par deux couches d'alvéoles opposées par leur fond. Dès l'Antiquité, on avait remarqué que les alvéoles ressemblaient à des prismes droits à base hexagonale régulière (voir la figure *Les alvéoles des abeilles*). Ce n'est qu'au XVIIIe siècle que l'on remarqua que le fond était l'assemblage de trois losanges identiques appartenant chacun à deux alvéoles opposées.

Un message y est caché. Lequel ?

Reconnaissance tardive La stéganographie a beau nous porter vers les délices de l'amour, le véritable sujet de ce livre est l'art de coder les informations, autrement dit la cryptologie. Malgré son importance manifeste sur les champs de bataille, ainsi que nous l'ont montré les échecs répétés des armées russes, cette science est rarement reconnue à sa juste valeur par les historiens. Pourquoi ? Tout simplement parce qu'elle est couverte par le secret. Ce n'est qu'en 1968, par exemple, que les historiens apprirent que les messages allemands de la Première Guerre mondiale (vous avez bien lu, la Première !) furent

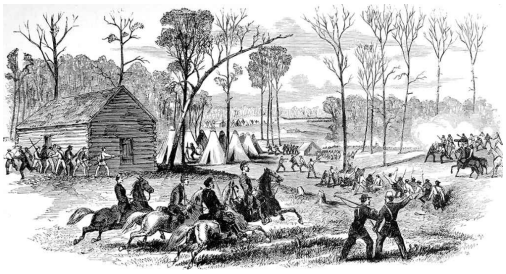
décryptés par les services français pratiquement tout au long du conflit… L'histoire était déjà écrite et personne ne s'était jamais vraiment soucié de creuser un sujet que les militaires eux-mêmes n'avaient pas exposé au grand jour.

La même discrétion a entouré les succès des Britanniques pendant la Seconde Guerre mondiale. En particulier grâce à la célèbre machine Enigma, eux aussi avaient su décrypter une grande partie des messages allemands, décidément guère appropriés pour dissimuler des secrets. Pourtant, les Britanniques ne s'en vantèrent pas, même après la guerre. Bien au contraire : jusqu'en 1973, ils prétendirent qu'Enigma était indécryptable, ce qui leur permit de revendre les machines confisquées à l'armée allemande auprès de gouvernements et d'entreprises étrangères !

Le César du meilleur chiffre Nous avons beaucoup parlé de cryptographie jusqu'ici, mais sans aborder encore d'exemple à proprement parler. Voyageons vers l'Antiquité pour ce premier contact avec la technique (qu'un enfant sachant lire peut déployer). Si je vous disais qu'à l'époque, l'un des hauts lieux de l'usage cryptographique était un territoire riche en ambitions militaires et en intrigues politiques, vous ne seriez pas étonné, n'est-ce pas ? Je veux bien entendu parler de Rome. Dans la biographie qu'il a consacrée aux douze Césars qui se sont succédé à la tête de la ville-empire (*Vies des douze Césars*), Suétone décrit une manière de chiffrer qu'utilisait Jules César (le seul et l'unique) :

> César […] employait, pour les choses tout à fait secrètes, une espèce de chiffre qui en rendait le sens inintelligible (les lettres étant disposées de manière à ne pouvoir jamais former un mot), et qui consistait, je le dis pour ceux qui voudront les déchiffrer, à changer le rang des lettres dans l'alphabet, en écrivant la quatrième pour la première, c'est-à-dire le D pour l'A, et ainsi de suite.

Reprenons l'exemple « FHFL HVW XQ PHVVDJH FRGH » que nous avons déjà rencontré plus haut. Je l'ai chiffré avec cette méthode. Ceux d'entre vous qui souhaitent se familiariser avec les techniques de cryptographie élémentaires sont invités à se faire la main dessus. Pour les autres, il suffit de décaler chaque lettre de trois lettres dans le sens opposé. Ainsi, F devient C, H devient E et ainsi de suite. En suivant ce procédé, on obtient le message (guère original) : « CECI EST UN MESSAGE CODE ». Si le pas de décalage vous était inconnu, vous auriez pu sans problème le déterminer par la méthode des fréquences.



Shiloh signifie « havre de paix » en hébreu, nom idéal pour une petite chapelle en rondins de bois… Ironie de l'Histoire, la bataille la plus meurtrière de la guerre de Sécession y débuta le 6 avril 1862 avec une offensive surprise des troupes sudistes. Elles avaient su garder le secret sur leur plan d'attaque en codant tout simplement leurs transmissions avec le chiffre de César ! Gravure de Frank Leslie, 1896.

Ce Qu'il Faut Décrypter Un message de César

Vercingétorix intercepte le message suivant de César à l'un de ses généraux :

DWWDT XHCDT XDWUH KHXUH VSDUO HQRUG.

Saurez-vous le décrypter ?

Malgré son ancienneté et sa simplicité (pour ne pas dire plus), le chiffre de César a été utilisé au moins deux fois à l'époque moderne. Étonnant, non ? Il faut croire que la facilité de mise en œuvre du code primait devant sa faiblesse. Ainsi, en 1862, avant la bataille de Shiloh pendant la guerre de Sécession, le général sudiste Albert Johnston, excellent officier mais piètre cryptologue, échangea avec son adjoint en recourant à un chiffre à décalage – avec succès semble-t-il puisque les nordistes furent pris par surprise. Ceux-ci tinrent toutefois leur revanche le lendemain et transformèrent la déroute initiale en victoire, au prix d'un coût humain terrible.

Au début de la Première Guerre mondiale, ce fut au tour de l'armée russe de se tourner vers le chiffre de César. Les généraux venaient de réaliser la nécessité de chiffrer leurs messages. Ce type de codage leur a sans doute été dicté par une armée mal formée et constituée de nombreux soldats illettrés. Comme nous l'avons évoqué au début de ce chapitre, il les mena à la défaite.

Chiffre ou code ?

Dans le récit biographique de Jules César, Suétone (ou plutôt son traducteur) use du terme de « chiffre » et non celui de « code ». Je l'ai moi-même employé plus ou moins indifféremment jusqu'ici. Il existe pourtant une différence subtile entre les deux termes. Un chiffre opère plutôt sur les unités élémentaires qui composent le message : lettres, syllabes, ou autres. En revanche, un code s'applique aux mots ou aux phrases du message, et sur leur signification.

Par exemple, dans le code des émoticônes, ☺ signifie « je suis content », ☹ le contraire. L'ensemble des codes est, en général, réuni dans un livre de codes, ainsi que nous le verrons avec les dictionnaires chiffrés au chapitre suivant.

La confusion entre chiffre et code n'est cependant pas bien grave et je privilégierai dans cet ouvrage le sens commun, qui tourne autour du secret.

Quand les deux techniques se volent dans les plumes

Je vous ai présenté la stéganographie et la cryptographie comme des méthodes séparées. Mais il est possible de les mêler, de la même manière que deux couleurs primaires se combinent pour produire une nouvelle couleur. Al-Moetamid Ibn Abad, le roi arabe de Séville de la fin XI^{e} siècle, nous en a fourni un exemple très visuel. Poète, il avait eu l'idée d'employer des noms d'oiseaux pour transmettre ses messages secrets. Chaque oiseau était associé à une lettre de l'alphabet. Al-Moetamid Ibn Abad commençait par dresser la liste des oiseaux correspondant aux lettres de son message, puis composait un poème à partir de cette litanie. Par exemple, si nous faisons correspondre les noms d'oiseaux à leur première lettre, en français, le poème :

> La tourterelle du matin craint le vautour, Qui pourtant préfère les nuées d'étourneaux, Ou au moins les loriots Qui, plus que tout, craignent les éperviers.

transmet le sinistre message : « tue-le » (j'ai un peu triché en faisant se confondre « u » et « v »). Ce type de code, où le message est caché tout en étant chiffré, se situe entre stéganographie et cryptographie.

Ce Qu'il Faut Décrypter Un message fleuri

Nous interceptons le message suivant :

Que de fleurs dans son jardin : campanules jaunes, églantiers, sauges de toutes les couleurs, œillets frisés, iris bleus, renoncules, narcisses, edelweiss si veloutés, véroniques, fumeterres, hortensias si rares, épilobes, violettes, roses, euphorbes et sarriettes au goût poivré.

Quel message caché véhicule-t-il ?

Les litanies de Trithème Héritier spirituel du roi de Sicile, l'abbé Jean Trithème (1462-1516) a, lui, imaginé un système de cryptographie dissimulé dans des litanies religieuses. À son époque les prières liturgiques constituaient un bon paravent pour dissimuler des messages. La liste des termes auquel il avait recours figure dans les tableaux ci-après. Les litanies sont en latin, mais il est inutile de maîtriser la langue pour utiliser le système, qu'on cherche à chiffrer un message ou à le déchiffrer. À chaque lettre de l'alphabet correspondent plusieurs mots ou phrases. Jean Trithème effectuait son choix parmi 18 possibilités, mais je n'ai donné ici que 8 en guise d'exemples.

A	Pater	Noster qui	Es in	Caelis
	Dominus	Nostrum qui	Gloriosus in	Celo
B				
	Creator	Omnium qui	Graditur in	Altis
C				
	Benefactor	Cunctorum qui	Extas in	Alto
D				
	Sanator	Universorum qui	Existis in	Exelsis

E				
F	Salvator	Chistianorum qui	Manes in	Exelso
G	Conservator	Predestinorum qui	Permanes in	Altissimo
H	Justificator	Supercolestium qui	Resplendes in	Altissumis
I	Adjutor	Universalium qui	Dominaris in	Celestibus
L	Auxiliator	Generatium qui	Luces in	Omnibus
M	Autor	Generis nostri qui	Principaris in	Universis
N	Index	Hominum qui	Triomphas in	Supernis
O	Rex	Justororum qui	Imperas in	Paradiso
P	Rector	Bonorum qui	Regnas in	Celesti
Q	Defensor	Piorum qui	Reluces in	Empireo

R	Imperator	Mitium qui	Sedes in	Aevum
S	Liberator	Fidelium qui	Resides in	Aeviternum
T	Vivificator	Sanctorum qui	Refulges in	Aeternum
V	Consolator	Credentium qui	Habitas in	Perpetuum
X	Magister	Angelorum qui	Rutilas in	Aeternitate
Y	Admonitor	Spiritum qui	Splendescis in	Eminentissimo
Z	Arbiter	Orthodoxorum qui	Glorificaris in	Supremis

A	Sanctificetur	Nomen tuum	Adveniat tuum	Regnum tuum
B	Magnificetur	Domicilium tuum	Conveniat tuum	Imperium tuum
C	Glorificetur	Aedificium tuum	Perveniat tuum	Dominium tuum
D	Benedicatur	Latibulum tuum	Proveniat tuum	Institutuum tuum

E	Honorificetur	Vocabulum tuum	Accedat tuum	Documentium tuum
F	Superexaltetur	Imperium tuum	Appropinquet tuum	Beneplacitum tuum
G	Honoretur	Regnum tuum	Magnificetur tuum	Repromissum tuum
H	Exaltetur	Scabellum tutum	Multiplicetur tuum	Constitutum tuum
I	Laudetur	Consilium tuum	Sanctificetur tuum	Promissum tuum
L	Oeiligatur	Eloquium tuum	Dilatetur tuum	Verbum tuum
M	Ametur	Institutum tuum	Pacificetur tuum	Dogma tuum
N	Adoretur	Constitutum tuum	Amplietur tuum	Ovile tuum
O	Colatur	Alloquium tuum	Proevaleat tuum	Opus tuum
P	Invocetur	Mysterium tuum	Convaleat tuum	Placitium tuum
	Celebretur	Testimonium tuum	Exaltetur tuum	Complacitum tuum

Q				
R	Collandetur	Evangelium tuum	Augeatur tuum	Promium tuum
S	Clarificetur	Cognomentum tuum	Firmetur tuum	Amuletum tuum
T	Beatificetur	Cognomen tuum	Confirmetur tuum	Adjutorium tuum
V	Manifestetur	Proenomen tuum	Crescat tuum	Remedium tuum
X	Agnoscatur	Pronomen tuum	Veniat tuum	Domicilium tuum
Y	Cognoscatus	Templium tuum	Veniens esto tuum	Testimonium tuum
Z	Notium esto	Agnomentum tuum	Crescens esto tuum	Sanctuarium tuum

Frottons-nous au message « ALERTE ». En accord avec les tableaux, une possibilité de litanie est :

Pater generatium qui existis in aevum beatificetur vocabulum tuum

La méthode de Trithème comporte un défaut : la longueur des messages produits. Sans compter que si la litanie tombe entre les mains d'un bon latiniste, elle ne vaudra plus tripette ! Nous retrouverons Trithème au sujet des substitutions poly-alphabétiques, dont ses litanies sont un premier exemple.

Ce Qu'il Faut Décrypter Une étrange prière

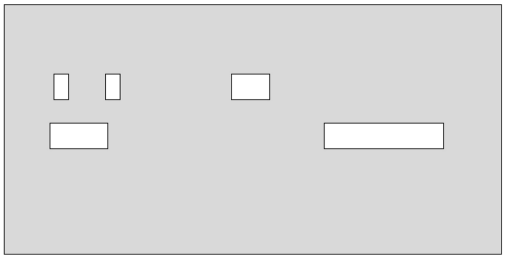
Un disciple de Jean Trithème propose une nouvelle prière :

Liberator noster qui habitas in perpetuum honnorificatur cognomen tuum proevaleat tuum promissum tuum.

Une idée du vrai message ?

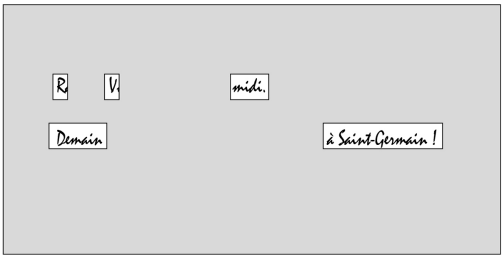
Bas les masques

Pour clore cette mise en bouche sur l'art de chiffrer les messages, je vous propose de faire tomber les masques. Littéralement. Notre histoire se déroulant en Italie, nous aurions pu partir pour le festival de Venise, mais dirigeons-nous plutôt pour Pavie où est né au XVIe siècle Girolamo Cardano, appelé Jérôme Cardan en France. Savant accompli, Cardan est surtout connu aujourd'hui pour sa résolution des équations du troisième degré et le fameux système de transmission pour véhicules qui porte son nom. Il fut également l'inventeur d'un dispositif, situé entre stéganographie et cryptographie, destiné à chiffrer des messages à l'aide d'une sorte de masque en forme de carte perforée. Pour communiquer de façon secrète, deux personnes doivent partager la même feuille de carton épais ou de métal, percée de cases rectangulaires.



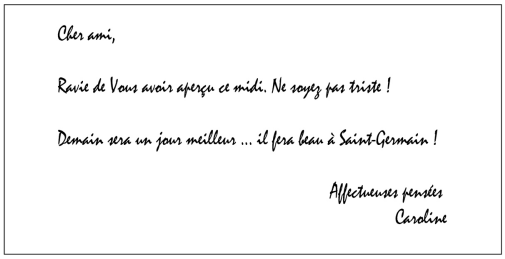
Une grille de Cardan.

Pour l'utiliser, on pose la grille sur une feuille de papier, puis on écrit le message secret dans les cases prévues. Par exemple, si on veut donner rendez-vous à son correspondant le lendemain midi à Saint-Germain, on écrira :



Écriture du message secret dans les cases.

On enlève alors la grille et on complète le message pour qu'il devienne naturel et anodin.


Cher ami,
Ravie de Vous avoir aperçu ce midi. Ne soyez pas triste !
Demain sera un jour meilleur ... il fera beau à Saint-Germain !
Affectueuses pensées
Caroline

On complète alors le message.

Le destinataire pose ensuite sa propre grille sur la lettre et révèle le message. Ce dispositif s'appelle une grille de Cardan. Coder un message de cette façon est un exercice de nature plus littéraire que scientifique. L'idée a cependant mené à une méthode cryptographique complexe à base de grilles tournantes que nous verrons plus tard. En attendant, les grilles de Cardan illustrent à quel point la cryptographie a de tout temps stimulé les imaginations. Quand d'aucuns n'y voyaient qu'un art guerrier, beaucoup y prenaient manifestement un certain plaisir !

2 La saga des dictionnaires chiffrés

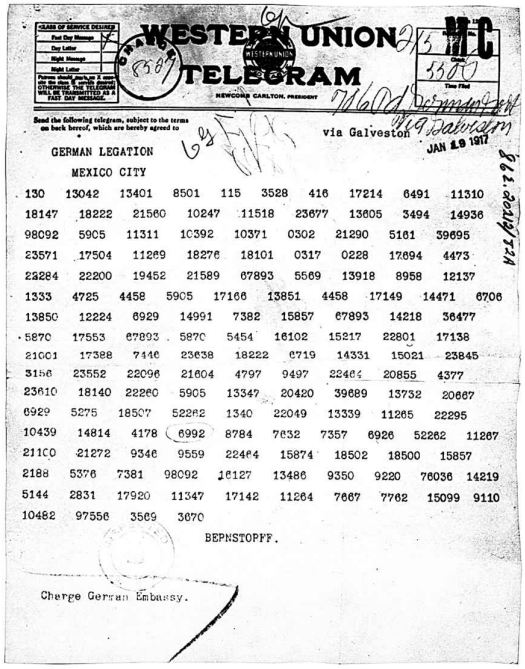
Alors que nous entamons tout juste cette aventure de la cryptographie ensemble, je dois vous poser une question qui peut sembler embarrassante : combien de codes du chapitre 1 êtes-vous parvenu à décrypter ? Un, deux, davantage ? Si votre réponse est zéro, rassurez-vous, je pense que vous appartenez à la majorité de lecteurs, qui parcourront cet ouvrage comme un livre d'histoire et non un ouvrage de mathématiques. En revanche, si vous avez réussi le grand chelem en cassant tous les codes, bravo ! Mais feriez-vous pour autant un bon cryptologue en temps de guerre ? Pas si sûr…

Au cours des derniers millénaires, la quasi-totalité des généraux d'armée ont commis la même faute : considérer que le décryptement était un défi posé à l'intelligence. « Mon code est inviolable, car personne sur terre n'est suffisamment intelligent pour en comprendre les arcanes » : telle était en substance leur pensée. Ce faisant, ils répétaient une erreur monumentale dont s'étaient déjà rendues responsables des générations de militaires avant eux. Heureusement qu'un cryptologue néerlandais de la fin du XIX^{e} siècle était là pour leur ouvrir les yeux…

Un curieux message

L'affaire, connue sous le nom de télégramme Zimmermann, va me servir à illustrer la faute commise. Le 23 février 1917, Arthur Balfour, ministre des Affaires étrangères du Royaume-Uni, reçut l'ambassadeur des États-Unis à Londres et lui remit un télégramme allemand. La missive avait transité par la Western Union, alors la plus importante société internationale de radiocommunication, et fut interceptée par les Britanniques de façon rocambolesque, comme je le préciserai plus loin. Si le télégramme était chiffré, il comportait aussi une partie compréhensible, formée de l'identité de l'expéditeur (l'ambassadeur d'Allemagne aux États-Unis) et du destinataire (l'ambassade d'Allemagne au Mexique).

Le reste du message était constitué d'une suite de 153 nombres de trois à cinq chiffres : « 130 13042 13401 8501 … 97556 3569 3670 ». Nul besoin d'être un fin stratège pour comprendre que si ce message s'avérait authentique, son contenu intéresserait les Américains. Selon les Britanniques, il avait été trouvé dans les locaux de la Western Union au Mexique par leur propre service d'espionnage. Les Britanniques avaient déjà cassé le code et livrèrent à l'ambassadeur américain ce qu'ils pensaient être la traduction correcte :



WESTERN UNION TELEGRAM

NEWCOMB CARLTON, PRESIDENT

Send the following telegram, subject to the terms on back hereof, which are hereby agreed to

via Galveston

JAN 19 1917

GERMAN LEGATION
MEXICO CITY

130 13042 13401 8501 115 3528 416 17214 6491 11310
18147 18222 21560 10247 11518 23677 13605 3494 14936
98092 5905 11311 10392 10371 0302 21290 5161 39695
23571 17504 11269 18276 18101 0317 0228 17694 4473
22284 22200 19452 21589 67893 5569 13918 8958 12137
1333 4725 4458 5905 17166 13851 4458 17149 14471 6706
13850 12224 6929 14991 7382 15857 67893 14218 36477
5870 17553 67893 5870 5454 16102 15217 22801 17138
21001 17388 7446 23638 18222 6719 14331 15021 23845
3156 23552 22096 21604 4797 9497 22464 20855 4377
23610 18140 22260 5905 13347 20420 39689 13732 20667
6929 5275 18507 52262 1340 22049 13339 11265 22295
10439 14814 4178 6992 8784 7632 7357 6926 52262 11267
21100 21272 9346 9559 22464 15874 18502 18500 15857
2188 5376 7381 98092 16127 13486 9350 9220 76036 14219
5144 2831 17920 11347 17142 11264 7667 7762 15099 9110
10482 97556 3569 3670

BEPNSTOPFF.

Charge German Embassy.

Texte original du télégramme Zimmermann.

Nous avons l'intention de déclencher à partir du premier février une guerre sous-marine totale. Malgré cela, nous tenterons de maintenir les États-Unis dans la neutralité. Si nous n'y parvenons pas, nous proposerons au Mexique une alliance sur les bases suivantes : faire la guerre ensemble, faire la paix ensemble, large soutien financier et accord de notre part pour la reconquête par le Mexique des territoires perdus du Texas, du Nouveau-Mexique et de l'Arizona. Le règlement des détails est laissé à vos soins. Vous informerez secrètement le président du Mexique dès que l'entrée en guerre des États-Unis sera certaine, et vous lui suggérerez que, sous sa propre initiative, il peut immédiatement solliciter la participation du Japon, et en même temps servir de médiateur entre le Japon et nous-mêmes. Prière d'attirer l'attention du président sur le fait que l'emploi sans limites de nos sous-marins offre désormais la possibilité d'obliger l'Angleterre à faire la paix dans peu de mois.

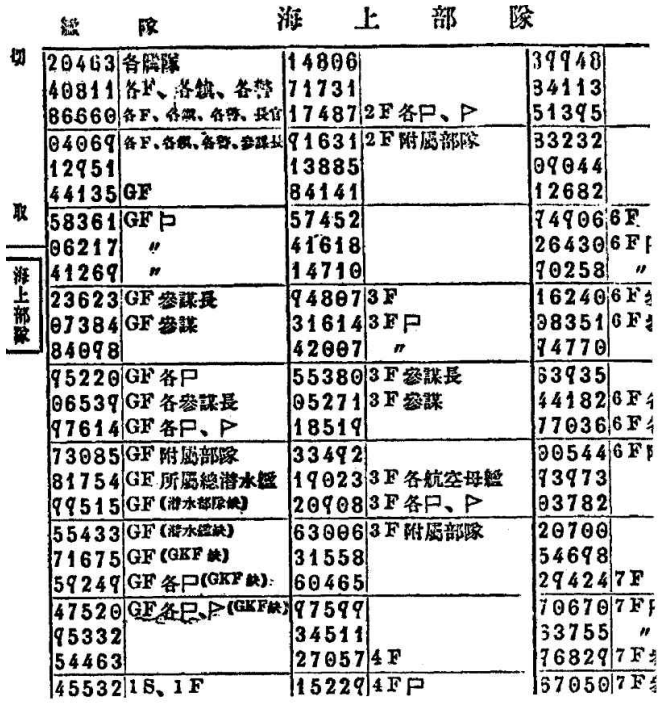
Signé : Zimmermann

Un tel texte, s'il émanait bien du ministre des Affaires étrangères allemand, Arthur Zimmermann, était de nature à pousser les États-Unis à entrer en guerre au côté des Alliés. Cette remarque rendait une manipulation britannique plausible. Nous verrons plus loin comment les Américains réussirent à exclure cette hypothèse.

Des chiffres et des lettres

Comment les Britanniques prétendaient-ils avoir cassé le code ? Selon eux, le premier nombre du télégramme (130) était une simple référence d'envoi, tandis que le deuxième (13042) fournissait le code utilisé, celui de la diplomatie allemande. Il faut savoir qu'à l'époque, les services de chiffrement se fondaient sur des dictionnaires chiffrés, c'est-à-dire des livres entiers faisant correspondre les mots de la langue d'origine du message avec des nombres à cinq chiffres ou moins. Évidemment, chaque service disposait de son propre dictionnaire chiffré. En France, depuis la loi française du 13 juin 1866 sur les usages commerciaux autorisant le chiffrement des dépêches privées, bon nombre de codes de ce type avaient vu le jour. Leur usage n'était pas seulement militaire, car leur essor avait accompagné le développement du télégraphe.

Combien de mots comportaient ces dicos ? Figurer les mots avec des nombres à cinq chiffres permettait en théorie de coder 100 000 mots, mais la plupart des dictionnaires n'en comptaient qu'environ 11 000, ce qui formait une pioche amplement suffisante pour communiquer. Ainsi, le chiffre de la marine japonaise JN-25 B (une appellation américaine, JN signifiant Japanese Navy) pendant la Seconde Guerre mondiale reposait sur un livre de 45 000 mots ou expressions (au passage, vous noterez que les dictionnaires chiffrés ne se limitaient pas aux langues s'écrivant à travers des alphabets).



艦隊		海上部隊			
20463	各艦隊	14806		39748	
40811	各F、各航、各警	71731		84113	
86660	各F、各艦、各隊、長官	17487	2F各戸、ト	51395	
04069	各F、各艦、各隊、参謀長	91631	2F附属部隊	83232	
12951		13885		09044	
44135	GF	84141		12682	
58361	GF戸	57452		74906	6F
06217	〃	41618		26430	6F
41269	〃	14710		70258	〃
23623	GF参謀長	94807	3F	16240	6F
07384	GF参謀	31614	3F戸	98351	6F
84098		42007	〃	74770	
95220	GF各戸	55380	3F参謀長	63935	
06539	GF各参謀長	05271	3F参謀	44182	6F
97614	GF各戸、ト	18519		77036	6F
73085	GF附属部隊	33492		90544	6F
81754	GF所属総潜水艦	19023	3F各航空母艦	73973	
99515	GF(潜水部隊長)	20908	3F各戸、ト	03782	
55433	GF(潜水艦隊)	63006	3F附属部隊	20700	
71675	GF(GKF隊)	31558		54698	
59249	GF各戸(GKF隊)	60465		29424	7F
47520	GF各戸、ト(GKF隊)	97599		70670	7F
95332		34511		33755	〃
54463		27057	4F	76829	7F
45532	1S、1F	15229	4F戸	67050	7F

Extrait du livre de code JN-25 B.

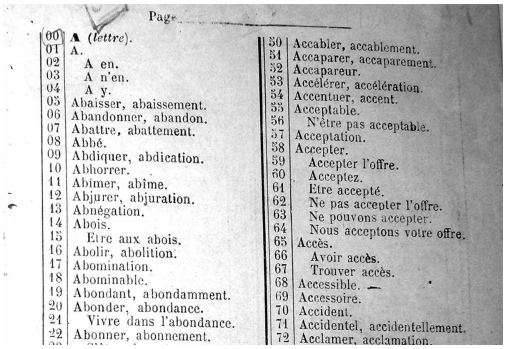
Le code de M. Tout-le-Monde

En France, le dictionnaire chiffré le plus connu fut le code Sittler, œuvre de F.-J. Sittler dont on ne sait rien, si ce n'est qu'il s'agissait d'un ancien fonctionnaire des services télégraphiques. L'ouvrage fut employé entre 1890 et 1920 par des particuliers comme par des entreprises et par l'Etat. Il tient en un petit livre dont la partie « code » est composée de cent pages. Chaque feuillet possédait un espace vierge en en-tête, afin de laisser le libre choix au lecteur de sa numérotation. Un long préambule expliquait la marche à suivre. En voici un extrait pour l'intérêt historique :

> Le dictionnaire chiffré, de F.-J. Sittler, composé dans le but de faciliter la rédaction et la traduction des dépêches secrètes, renferme à peu près tous les mots et expressions d'un usage fréquent. Pour employer le langage secret, au moyen de ce Dictionnaire, il suffit d'indiquer à son correspondant la page et la ligne où se trouve le mot ou l'expression que l'on veut lui transmettre. À cet effet, on adopte d'un commun accord, une pagination conventionnelle, en employant, dans un ordre quelconque, les numéros

depuis 00 jusqu'à 99, et une combinaison également conventionnelle des deux chiffres de la page avec ceux de la ligne.
Exemple : Supposons que la première page reçoive le n° 82, l'expression : « Nous acceptons votre offre, » ligne 64 (voir l'extrait de la première page), sera représentée : par 8264 ou 6482 ou 8624 ou 6824 etc. C'est-à-dire que la page sera représentée, ou par les deux premiers chiffres ou par les deux derniers, ou par le 1er et le 3e, ou par le 2e et le 3e, etc., et la ligne par les deux autres. On peut aussi, d'un commun accord, augmenter ou diminuer d'une ou de plusieurs unités, un quelconque des 4 chiffres du groupe.

L'opération décrite à la fin de ce passage (permutation des chiffres, augmentation ou diminution du code) est appelée un surchiffrement. Elle consiste à ajouter un codage supplémentaire au chiffre initial. C'est un moyen de renforcer la complexité de l'ensemble. Les Allemands usaient souvent de ce stratagème : un des derniers chiffres transmis indiquait alors la correction à apporter. Par exemple, le nombre 0183 placé à la fin pouvait indiquer « augmenter tous les codes de 183 ».


Page

00	A (*lettre*).
01	A.
02	A en.
03	A n'en.
04	A y.
05	Abaisser, abaissement.
06	Abandonner, abandon.
07	Abattre, abattement.
08	Abbé.
09	Abdiquer, abdication.
10	Abhorrer.
11	Abîmer, abîme.
12	Abjurer, abjuration.
13	Abnégation.
14	Abois.
15	Etre aux abois.
16	Abolir, abolition.
17	Abomination.
18	Abominable.
19	Abondant, abondamment.
20	Abonder, abondance.
24	Vivre dans l'abondance.
22	Abonner, abonnement.
50	Accabler, accablement.
51	Accaparer, accaparement.
52	Accapareur.
53	Accélérer, accélération.
54	Accentuer, accent.
55	Acceptable.
56	N'être pas acceptable.
57	Acceptation.
58	Accepter.
59	Accepter l'offre.
60	Acceptez.
61	Etre accepté.
62	Ne pas accepter l'offre.
63	Ne pouvons accepter.
64	Nous acceptons votre offre.
65	Accès.
66	Avoir accès.
67	Trouver accès.
68	Accessible.
69	Accessoire.
70	Accident.
71	Accidentel, accidentellement.
72	Acclamer, acclamation.

Extrait de la première page du code Sittler. En lui attribuant le numéro 62, le message « Nous acceptons votre offre » se codait 6264 (sans surchiffrement).

Le code de Sittler possédait un avantage par rapport à d'autres dictionnaires chiffrés, ce qui a expliqué son succès commercial : il permettait d'obtenir des messages plus courts, donc moins onéreux. Pour obtenir le compte des mots d'une dépêche télégraphique chiffrée, il fallait diviser en effet la somme totale des chiffres par 5. Par exemple 25

groupes de 4 chiffres ne comptaient que pour 20 mots. Pourquoi, direz-vous ? Il s'agit juste de la règle de découpage des messages télégraphiés. On retrouvera ce découpage en 5 dans tout cet ouvrage.

Une affirmation péremptoire

À la fin de son texte de présentation, Sittler affirmait un peu vite qu'il était « facile de se convaincre qu'on peut ainsi créer un nombre infini de clefs absolument indéchiffrables ». Cette allégation venait de la possibilité de numéroter les pages et du surchiffrement : même en disposant du livre de code, comment un œil indiscret aurait-il pu deviner la numérotation des pages et la permutation utilisée ? se disait Sittler. *A priori*, il avait parfaitement raison…

Sauf que Sittler oubliait que, bien longtemps avant lui, un scientifique italien de la Renaissance, Giambattista della Porta (1535-1615), considéré par certains comme le père de la cryptographie, avait justement inventé une méthode pour déterminer ce genre de fioritures. Elle consiste à chercher un mot dont la présence est probable dans le message. Il en existe presque toujours, par exemple les noms propres qui doivent être épelés ou divisés en syllabes ou en mots du dictionnaire.

Pour comprendre comment mettre l'idée en pratique, considérons à titre d'exemple le message suivant, chiffré avec le code de Sittler : « 0726 0728 1564 ». Imaginons qu'on sache qu'il concerne une personne nommée Abélard. Ce nom ne figurant pas dans le dictionnaire, une hypothèse plausible est qu'il soit codé grâce aux deux mots « abbé » et « lard », soit 08 dans une page (la première) et 14 dans une autre. Un examen rapide de la suite de chiffres du message montre que 08 et 14 se trouvent en première et dernière place des deux derniers groupes. Ainsi, 72 et 56

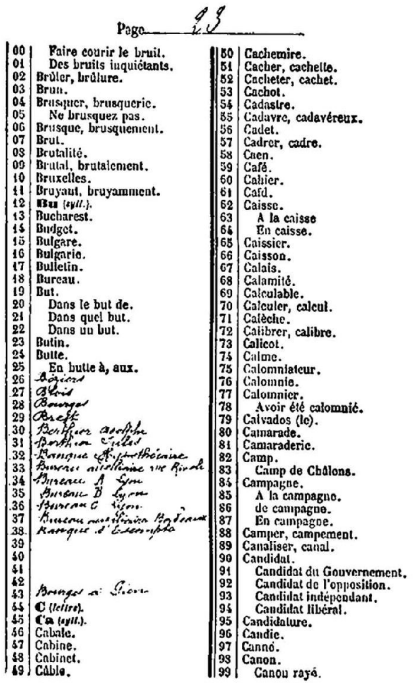
seraient les numéros des pages correspondantes. Le sens du mot 06 de la page codée 72 est donc « abandonner ».

Avec ces hypothèses, on en conclut que le message signifie « abandonner Abélard ». La technique s'appelle aujourd'hui la méthode du mot probable. Bien entendu, j'ai simplifié à l'extrême l'exemple pour la clarté de la démonstration. Le travail des vrais décrypteurs militaires était autrement plus complexe, comme va nous le montrer un célèbre scandale historique : l'affaire Dreyfus.

Ce Qu'il Faut Décrypter

Message à Abélard

Vous interceptez le message suivant destiné à Abélard : « 0828 1234 6824 ».
Vous suspectez qu'il a été chiffré avec le livre de code de Sittler. Sous cette hypothèse, saurez-vous le décrypter ?



Page 93

00 Faire courir le bruit.
01 Des bruits inquiétants.
02 Brûler, brûlure.
03 Brun.
04 Brusquer, brusquerie.
05 Ne brusquez pas.
06 Brusque, brusquement.
07 Brut.
08 Brutalité.
09 Brutal, brutalement.
10 Bruxelles.
11 Bruyant, bruyamment.
12 Bsu (syll.).
13 Bucharest.
14 Budget.
15 Bulgare.
16 Bulgarie.
17 Bulletin.
18 Bureau.
19 But.
20 Dans le but de.
21 Dans quel but.
22 Dans un but.
23 Butin.
24 Butte.
25 En butte à, aux.
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44 C (lettre).
45 C'a (syll.).
46 Cabale.
47 Cabine.
48 Cabinet.
49 Câble.
50 Cachemire.
51 Cacher, cachette.
52 Cacheter, cachet.
53 Cachot.
54 Cadastre.
55 Cadavre, cadavéreux.
56 Cadet.
57 Cadrer, cadre.
58 Caen.
59 Café.
60 Cahier.
61 Caïd.
62 Caisse.
63 A la caisse
64 En caisse.
65 Caissier.
66 Caisson.
67 Calais.
68 Calamité.
69 Calculable.
70 Calculer, calcul.
71 Calèche.
72 Calibrer, calibre.
73 Calicot.
74 Calme.
75 Calomniateur.
76 Calomnie.
77 Calomnier.
78 Avoir été calomnié.
79 Calvados (le).
80 Camarade.
81 Camaraderie.
82 Camp.
83 Camp de Châlons.
84 Campagne.
85 A la campagne.
86 de campagne.
87 En campagne.
88 Camper, campement.
89 Canaliser, canal.
90 Candidat.
91 Candidat du Gouvernement.
92 Candidat de l'opposition.
93 Candidat indépendant.
94 Candidat libéral.
95 Candidature.
96 Candie.
97 Canné.
98 Canon.
99 Canon rayé.

Une page d'un exemplaire (utilisé) du code Sittler. On notera la pagination (23), ainsi que l'ajout de mots importants pour l'utilisateur : des noms de villes et de bureaux, sans doute ceux d'une entreprise.

Le code Baravelli et l'affaire Dreyfus

L'affaire Dreyfus bouscula la Troisième République et révéla une face sombre de la France de l'époque. Sans revenir sur cette affaire dans les détails, je me contenterai de rappeler le minimum nécessaire à la compréhension de la suite. En 1894, le capitaine Alfred Dreyfus (1859-1935) fut accusé d'espionnage au profit de l'Allemagne et de l'Italie, alors alliées à l'Autriche-Hongrie dans le cadre de la Triple Alliance, ou Triplice. La seule « preuve » matérielle contre lui était la ressemblance de son écriture avec celle de l'espion véritable, qui fut démasqué plus tard. L'affaire fit très vite grand bruit dans la presse, si bien que l'attaché militaire italien se sentit obligé d'en rendre compte à son gouvernement. Il adressa à Rome un télégramme, bien entendu chiffré puisqu'il passait par la poste française. Le voici :

> Paris, le 2 novembre 1894, 3 heures du matin Commando Stato Maggiore Roma
> 913 44 7836 527 3 88 706 6458 71 18 0288 5715 3716 7567 7943 2107 0018 7606 4891 6165

Comme pour tous les télégrammes chiffrés de l'époque, un double fut aussitôt transmis au ministère français des Affaires étrangères français. Son meilleur décrypteur était alors Étienne Bazeries, dont nous avons déjà évoqué le génie (et que nous continuerons de souligner à propos des messages chiffrés du *Figaro* et du Grand Chiffre de Louis XIV). À cause de son découpage en groupes de 1, 2, 3 ou 4 chiffres, les décrypteurs du ministère pensèrent immédiatement à un code commercial utilisé en Italie, le *Dizionario per corripondenze in cifra* de Paolo Baravelli, dont la conception différait légèrement du code Sittler puisqu'il était divisé en quatre sections, la première en un chiffre, la deuxième en deux, etc.

Plus précisément, la première section comportait les dix chiffres (de 0 à 9), qui codaient les voyelles et les signes de ponctuation. L'utilisateur pouvait modifier l'attribution des chiffres. La section suivante (de 00 à 99) correspondait aux consonnes, aux indications grammaticales et aux verbes auxiliaires. Il était possible de changer la distribution des chiffres des dizaines. La troisième section comportait dix pages correspondant aux syllabes et la quatrième section à des mots et expressions. Pour ces deux sections, la pagination était libre.

Un doute qui coûte cher

Revenons à notre message et essayons de le déchiffrer en appliquant la méthode du mot probable venue de la Renaissance italienne. Cherchons un nom propre. Le mot « Dreyfus » vient naturellement à l'esprit. Qui se traduit, avec le code de Baravelli, par le nombre (sans changement de pagination) « 227 1 98 306 ». Cette suite de chiffres évoque le passage « 527 3 88 706 » du message. En procédant de

même et en poursuivant le raisonnement, les décrypteurs révélèrent l'intégralité du message, au détail près qu'ils ne parvinrent pas à lever une ambiguïté sur un passage. Ils hésitaient entre deux versions. Malheureusement pour Dreyfus, le ministère des Affaires étrangères pencha d'abord pour la première, dont voici la traduction française :

> Si le capitaine Dreyfus n'a eu aucune relation avec vous, il serait opportun que l'ambassadeur l'affirme officiellement. Notre émissaire est prévenu.

Il la transmit au ministère de la Guerre, avant de se reprendre et de proposer cette nouvelle traduction :

> Si le capitaine Dreyfus n'a pas eu de relations avec vous, il conviendrait de faire publier par l'ambassadeur un démenti officiel pour éviter les commentaires de la presse.

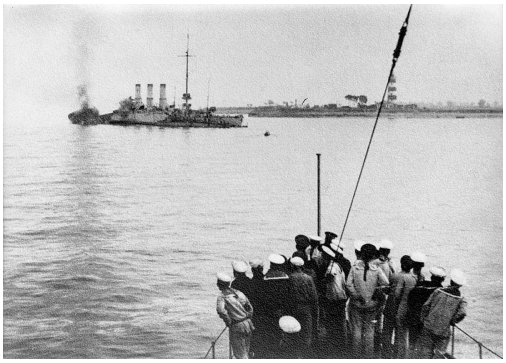
La seconde version est plus forte et indique clairement que Dreyfus n'a eu aucun contact avec l'attaché militaire italien, ce qui l'innocente, tandis que la première, pourtant comparable, peut laisser planer un doute.

Pour le lever, le service de renseignements du ministère de la Guerre eut l'idée de pousser les Italiens à chiffrer un message : le résultat dirait laquelle des deux solutions était la bonne, et apporterait aussi des informations complémentaires sur la pagination de leur dictionnaire chiffré. Un agent double fut chargé de communiquer à l'attaché italien des renseignements militaires paraissant de la première importance, qui se dépêcha de les chiffrer et de les envoyer via un télégramme, bientôt intercepté.

C'est grâce à ce subterfuge que les Français surent que la seconde solution était la bonne : Dreyfus, inconnu des Italiens, était donc innocent. Ce qui n'empêcha pas la hiérarchie militaire de camper sur sa position et de continuer à accuser à tort l'officier. Toutefois, en montrant le manque d'objectivité de la hiérarchie militaire, cet épisode fut plus tard un élément décisif dans la réhabilitation du capitaine.

Les faiblesses des dictionnaires chiffrés

Quelle conclusion tirer de l'affaire Dreyfus ? Qu'en dépit de ce que prétendait Sittler sur l'impossibilité de décrypter son code, nous voyons qu'utilisé tel quel… il n'est guère solide. Cela n'empêchait pas les autorités diplomatiques italiennes et allemandes d'employer des codes similaires. À ce propos, on peut s'étonner de voir des services gouvernementaux recourir à un code commercial que tout un chacun peut se procurer ! C'est d'autant plus étrange que les messages diplomatiques ou militaires fourmillent de mots à la probabilité d'occurrence importante : noms propres, ambassadeur, consul, général, colonel, armée, corps, division, régiment, homme, fusil, canon, etc. En cas de guerre, il est illusoire d'imaginer qu'un dictionnaire chiffré puisse échapper à l'ennemi, comme les Allemands l'ont appris à leurs dépens pendant la Première Guerre mondiale…



Le croiseur *Magdeburg*, échoué près de l'île d'Odensholm, sur lequel on trouva les livres de codes de la marine allemande. Les soldats allemands avaient l'ordre de les détruire en cas de situation désespérée, mais l'intervention de la marine russe ne leur en laissa pas le temps.

Août 1914, l'Allemagne vient d'entrer en guerre et le croiseur léger *Magdeburg* patrouille en mer Baltique pour y poser des mines. Le 26, un épais brouillard gêne la

navigation et le navire s'échoue près de l'île d'Odensholm. Sachant son bâtiment perdu, le commandant se résout à faire évacuer le navire et ordonne à un officier de prendre un bateau et d'aller jeter les livres de codes dans la mer profonde. Sage décision, compte tenu que deux croiseurs russes se profilent à l'horizon. Hélas pour les Allemands, le plan a des ratés. Les Russes commencent à tirer et, après une courte bataille, repêchent les vivants et les morts, dont l'officier qui tient les livres serrés dans ses bras…

Ces ouvrages furent plus tard remis à Winston Churchill, alors premier lord de l'Amirauté. Il s'agissait de dictionnaires chiffrés désordonnés. De plus, les codes correspondant à chaque mot n'étaient pas des numéros, mais des groupes de quatre lettres ; enfin, l'ordre (lexicographique) des codes ne suivait pas celui des mots qu'ils codaient. Même si tomber dessus constituait une véritable aubaine pour les Britanniques, il fallut malgré tout plusieurs semaines aux cryptanalystes de la Chambre 40, le service de décryptement de la marine britannique, pour exploiter la trouvaille. D'une complexité supérieure aux codes commerciaux que nous avons vus, les codes allemands étaient en effet surchiffrés au moyen d'une substitution mono-alphabétique pour la flotte de surface (voir le chapitre 4) et par une transposition pour les sous-marins (voir le chapitre 6).

Grâce à cette pêche miraculeuse, les Britanniques décryptèrent ensuite régulièrement les messages de la marine allemande. De façon surprenante, les Allemands ne se doutèrent de rien et ne changèrent de code qu'après la bataille du Jutland en 1916, quand, à force de trouver des unités de la marine britannique systématiquement sur leur chemin, ils cessèrent de croire à des coïncidences.

Un dictionnaire dans une valise

Un autre inconvénient majeur des dictionnaires chiffrés, quand ils sont ordonnés comme le 13040 – celui du télégramme Zimmerman –, est de permettre un décryptement progressif. Par exemple, si nous savons que « 23500 » signifie « jeudi » et « 23509 », « joie », le sens de 23504 se trouve entre les deux dans un dictionnaire usuel. Mais il est vrai que sans le livre du code 13040, il demeure difficile et long de décrypter un message qui a été chiffré avec.

Dans l'épisode du télégramme Zimmermann (qui contribua en 1917 à faire entrer en guerre les États-Unis), les Britanniques en possédaient bien un exemplaire. L'anecdote qui en explique la raison est plus rocambolesque que la malheureuse aventure du *Magdeburg*. Je vais l'évoquer rapidement car elle révèle une erreur fréquente en matière de secret. Elle met en scène Wilhelm Wassmuss, un diplomate allemand en poste en Perse au début du XX^{e} siècle.

À l'époque, la Perse était un territoire en principe neutre et indépendant, mais en réalité partiellement sous influence britannique. Wassmuss essayait d'y fomenter une guérilla antibritannique (comme Lawrence d'Arabie y parvint contre l'Empire ottoman dans les pays arabes). Conscients du danger, en 1915, les Britanniques demandèrent à des chefs de tribus persanes de le leur livrer, moyennant une prime bien sûr. Ceux-ci le capturèrent, mais il réussit à s'échapper pendant qu'ils négociaient le montant de la rançon ! Dans sa fuite, il abandonna ses bagages… qui se révélèrent renfermer le fameux dictionnaire chiffré 13040. C'est grâce à cette prise de guerre que le télégramme Zimmermann fut plus tard décrypté – enfin, selon la version officielle.

Wilhelm Wassmuss (1880-1931), surnommé Wassmuss de Perse, était un héros romantique de la trempe de Lawrence d'Arabie. Comme ce dernier, il parlait la langue du pays où il opérait et aimait s'habiller à la façon des autochtones. Les liens qu'il avait noués avec les tribus iraniennes cessèrent quand il devint évident que les Allemands ne gagneraient pas la guerre. En perdant les codes diplomatiques de son pays, il permit aux Britanniques de décrypter une partie des messages ennemis.

Les dictionnaires chiffrés désordonnés

Pour comprendre, je vous remets en mémoire rapidement l'affaire du télégramme : en 1917, les Britanniques remettent aux Américains un télégramme, prétendument allemand, annonçant leur intention prochaine de livrer une guerre sous-marine totale. Les Américains croient d'abord à une contrefaçon des services d'espionnage britanniques, destinée à les faire entrer en guerre, avant finalement de leur faire confiance. Or nous savons aujourd'hui que, même si le télégramme était authentique, les Britanniques ont effectivement manipulé leurs amis américains : ils l'avaient intercepté plus tôt qu'ils ne l'avaient prétendu… en

espionnant non pas les Allemands ou les Mexicains, mais les Américains !

En effet, ces derniers permettaient aux Allemands de communiquer à travers leur réseau pour faciliter les pourparlers de paix. Les scrupules étant hors de mise en période de guerre, les Allemands avaient fait transiter le télégramme Zimmermann par l'ambassade des États-Unis à Berlin, en le codant au moyen du code 0075, plus récent et réputé plus sûr que le 13040 (celui que contenait la valise du Lawrence d'Arabie perse). Les mots y étaient codés dans le désordre, ce qui interdisait l'interpolation entre deux mots découverts.

Ces livres de code désordonnés ont été employés jusque dans les années 1970 dans la diplomatie. Chacun comprenait deux gros livres, l'un étant la partie chiffrante, l'autre la partie déchiffrante. En guise d'exemple, voici une page du *Code Empire, modifié 67* servant aux les échanges dans l'empire français.

18018 **DISCRÉDIT** -er -é
57794 **DISCRET** -ement
08953 DISCRÉTion -ionnaire
29147 **DISCRIMIN**ation
75637 DISCRIMINer -é -ant
45977 **DISCULP**er -é -ation
33883 **DISCUSSION,** *de, d', du, de l', de la, des*
04553 ———— du projet, *de*
19108 **DISCUT**able
79448 DISCUTer -é
64764 **DISERT**
87952 **DISETTE**
00367 **DISGRAC**e -ier -ié -ieux
39662 **DISJOIN**dre -t
00627 **DISJONCT**eur -ion
10011 **DISLO**cation
46884 DISLOQUer -é
58840 **DISPACH**e -eur
05145 **DISPAR**aissant

Une page du *Code Empire*, modifié en 1967.

On y remarque que les numéros ne sont pas dans l'ordre et qu'il était possible d'y ajouter des mots non prévus à l'origine. Dans l'exemple suivant, le mot « discriminatoire » n'était pas prévu et a été ajouté en 1967.

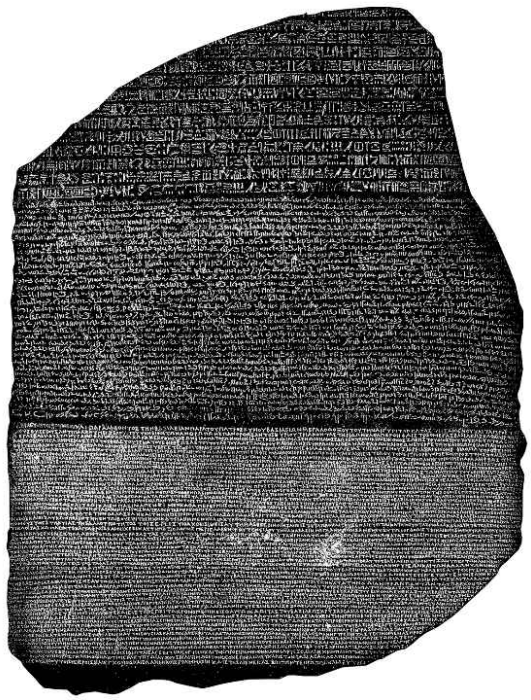
L'intelligence au service des Britanniques

Quand l'affaire du télégramme Zimmermann éclata, les Britanniques disposaient d'une partie du livre de code 0075, dénichée à bord d'un sous-marin ennemi au début de la guerre. Grâce à ce savoir, ils comprirent le sens général du télégramme dès son interception, fin janvier 1917. Cependant, deux raisons les empêchaient de le divulguer immédiatement à leurs amis américains. Premièrement, ils ne voulaient pas révéler aux Allemands qu'ils savaient lire leurs messages codés avec le 0075. Deuxièmement, il aurait été maladroit de montrer aux Américains qu'ils les espionnaient… Voyons comment les Britanniques surent contourner ces obstacles.

Le télégramme étant destiné à l'ambassadeur d'Allemagne au Mexique, et non à celui de Washington, ils pensèrent qu'il serait transféré par voie télégraphique de l'un à l'autre. Un double devait se trouver à l'agence de la Western Union à Mexico. C'est pourquoi ils demandèrent à leur espion en place de se le procurer. Chance incroyable, mais prévisible puisque toutes les ambassades ne disposaient pas des codes modernes : cette version du télégramme se révéla chiffrée avec le vieux 13040. Non seulement il n'était plus nécessaire de produire le texte codé avec le 0075 et donc de révéler que les services britanniques savaient partiellement le décrypter, mais, de plus, ce même texte chiffré avec deux codes différents fournissait un outil supplémentaire pour percer les secrets du code 0075 !

La pierre de Rosette des codes

Le télégramme Zimmermann joua ainsi le rôle que la pierre de Rosette tint jadis pour le déchiffrage des hiéroglyphes égyptiens (cette table de granit présentait trois versions du même texte en grec, en démotique et en hiéroglyphes, et Champollion se servit de cette correspondance pour comprendre l'antique langue écrite égyptienne). Pendant la Seconde Guerre mondiale, les Allemands systématisèrent cette erreur en envoyant les mêmes messages météorologiques selon divers canaux, offrant ainsi une avalanche de pierres de Rosette aux décrypteurs britanniques. Nous verrons que l'armée napoléonienne fit pire, en envoyant les mêmes portions de messages en clair et en chiffres…



La pierre de Rosette est un morceau de stèle de l'Égypte ancienne sur laquelle est gravé un même texte dans trois langues : grec, démotique (qui deviendra le copte) et hiéroglyphes. Elle a été découverte durant la campagne d'Égypte lors de travaux de terrassement dans une ancienne forteresse turque, où elle avait été employée comme matériau de construction. Grâce à son excellente

connaissance du grec ancien et du copte, Jean-François Champollion parvint en 1822 à la décrypter et à enfin percer le sens des hiéroglyphes. La pierre se trouve aujourd'hui au British Museum, à Londres.

La clef du problème

Nous voilà enfin parvenus à la faute grave qu'ont commise la quasi-totalité des généraux depuis des millénaires : croire que le décryptement est seulement un défi posé à l'intelligence. « Voilà mon message chiffré, arrachez-vous les cheveux pour le décoder », semblaient dire les militaires à leurs ennemis. Sauf qu'en raisonnant ainsi, ils oubliaient que la sécurité d'un système cryptographique ne peut reposer sur le seul secret de la méthode de chiffrement. Il ne faut jamais croire un code inviolable : voilà la règle à laquelle ils auraient dû s'astreindre. L'histoire du télégramme de Zimmermann, comme celle du message de Panizzardi, montre qu'un espion ou les hasards de la guerre peuvent toujours révéler l'algorithme mobilisé.

En fait, pour être sûr, un système cryptographique doit dépendre d'un paramètre facilement modifiable : sa clef. Ce principe a été formalisé par le cryptologue Auguste Kerckhoffs (1835-1903) en 1883, soit avant la Première Guerre mondiale ! Je ne résiste pas au plaisir de vous citer Kerckhoffs lui-même, qui se montrait d'une clairvoyance absolue, trente ans avant les échecs russes et allemands. Dans la première phrase du texte qui suit, il fait référence aux dictionnaires chiffrés tel le code Sittler, en vogue à l'époque :

> Il faut bien distinguer entre un système d'écriture chiffrée, imaginé pour un échange momentané de lettres entre quelques personnes isolées, et une méthode de cryptographie destinée à régler pour un temps illimité la correspondance des différents chefs d'armée entre eux. Ceux-ci, en effet, ne peuvent, à leur gré et à un moment donné, modifier leurs conventions ; de plus, ils ne doivent jamais garder sur eux aucun objet ou écrit qui soit de

nature à éclairer l'ennemi sur le sens des dépêches secrètes qui pourraient tomber entre ses mains.
Un grand nombre de combinaisons ingénieuses peuvent répondre au but qu'on veut atteindre dans le premier cas ; dans le second, il faut un système remplissant certaines conditions exceptionnelles, conditions que je résumerai sous les six chefs suivants :
1. Le système doit être matériellement, sinon mathématiquement, indéchiffrable ;
2. Il faut qu'il n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi ;
3. La clef doit pouvoir en être communiquée et retenue sans le secours de notes écrites, et être changée ou modifiée au gré des correspondants ;
4. Il faut qu'il soit applicable à la correspondance télégraphique ;
5. Il faut qu'il soit portatif, et que son maniement ou son fonctionnement n'exige par le concours de plusieurs personnes ;
6. Enfin, il est nécessaire, vu les circonstances qui en commandent l'application, que le système soit d'un usage facile, ne demandant ni tension d'esprit ni la connaissance d'une longue série de règles à observer.

Le premier emblème de l'organisation Volapük (vers 1880). *Menad bal – Pük bal*, soit « Une humanité – une langue ». Brillant cryptologue, Auguste Kerckhoffs s'était passionné pour cette langue construite, à visée internationale. Il y consacrera un *Cours complet,* puis un *Dictionnaire,* avant de fonder l'Association française pour la diffusion du Volapük.

Comment traduire aujourd'hui ces règles ? La quatrième devrait être remplacée par la correspondance sur Internet ou tout autre réseau public. Les deux dernières pourraient simplement relever d'un « fonctionnement automatisé ». Hormis ces détails, le principe de Kerckhoffs est toujours d'actualité. On pourrait le résumer en disant que, dans un bon chiffre, l'éventualité que l'ennemi connaisse le système ne doit pas affecter sa sécurité. Autrement dit, quand on

conçoit un algorithme cryptographique, mieux vaut partir de l'hypothèse : « L'ennemi connaît le système. » Cette dernière formulation est due à Claude Shannon (1916-2001), un grand mathématicien et cryptologue que nous retrouverons.

Décrypter sans connaître le dictionnaire

Le défaut principal des dictionnaires chiffrés est là : plus on connaît de mots du livre de codes, plus le secret des messages est facile à percer. Souvent, les gens pensent que seule la chance ou un acte d'espionnage révèlent la solution d'un message codé avec un dictionnaire. Comme les décrypteurs se vantent rarement de leurs exploits en public, cette croyance est assez courante. On la trouve même sous la plume du grand sceptique qu'était Voltaire, dans son *Dictionnaire philosophique* (paru en 1764), à l'article « poste ». Voltaire y explique d'abord l'origine de la cryptographie et l'erreur qui consiste à mêler clair et chiffre :

> Pour dérouter l'empressement des curieux, on imagina d'abord d'écrire une partie de ses dépêches en chiffres ; mais la partie en caractères ordinaires servait quelquefois à faire découvrir l'autre.

Logiquement, il note ensuite que cela développa l'art du chiffrement comme celui du décryptement. Pour autant, il conclut en considérant le décryptement comme impossible dès lors qu'un chiffre est bien fait, fort d'un raisonnement que nous retrouverons tout au long de l'Histoire, en particulier avec Enigma : le grand nombre de possibilités. Ce en quoi Voltaire se trompe, car les décrypteurs n'ont nullement besoin d'essayer toutes les possibilités !

Voici le texte de Voltaire, avec toute la saveur de la langue de l'époque :

> On opposa à ces énigmes l'art de les déchiffrer mais cet art fut très fautif et très vain. On ne réussit qu'à faire accroire à des gens peu instruits qu'on avait déchiffré leurs lettres ; et on n'eut que le plaisir de leur donner des

> inquiétudes. Telle est la loi de probabilités que dans un chiffre bien fait il y a deux cents, trois cents, quatre cents à parier contre un, que dans chaque numéro vous ne devinerez pas la syllabe dont il est représentatif.
> Le nombre des hasards augmente avec la combinaison de ces numéros et le déchiffrement totalement impossible quand le chiffre est fait d'un peu d'art. Ceux qui se vantent de déchiffrer une lettre sans être instruits des affaires qu'on y traite et sans des secours préliminaires sont de plus grands charlatans que ceux qui se vanteraient d'entendre langue qu'ils n'ont point apprise.

Cette croyance de Voltaire a pu être alimentée par le sort du chevalier de Rohan (1635-1674) qui se vantait de savoir lire n'importe quel message chiffré sans en posséder la clef. Une forfanterie qui lui fit perdre la tête, suite à une lourde méprise. Soupçonné d'avoir participé à une conspiration ourdie contre Louis XIV, le chevalier était enfermé à la Bastille dans l'attente de son jugement lorsque ses amis lui envoyèrent un paquet de chemises contenant un message chiffré, inscrit sur la manche de l'une d'elles :

> MG DULHXCCLGU GHJ YXUJ LM CT ULGE ALJ

Le mot le prévenait qu'aucune charge n'existait contre lui, l'instigateur du complot étant mort sans rien avoir révélé de sa complicité. Mais, incapable de traduire le message par totale incompétence, Rohan fut pris de peur. S'imaginant qu'on voulait l'informer de la découverte de preuves contre lui, il avoua tout à ses juges le lendemain. Il fut condamné et décapité. Le message n'avait pourtant été chiffré que par une simple substitution alphabétique, une méthode simple à briser…

L'homme au masque de fer

Répétons-le, nul besoin de chance, voire de mettre la main sur un dictionnaire chiffré pour décoder le message. Il existe des techniques pour casser le code. Nous en avons déjà vu une : l'analyse fréquentielle, c'est-à-dire l'observation des répétitions que l'on peut mettre en

parallèle avec celles des lettres d'un texte. Le fameux cryptologue de la fin du XIXe siècle Étienne Bazeries en employa une autre, avec laquelle, il réussit à casser le « Grand Chiffre de Louis XIV ». Ce chiffre avait été conçu trois cents ans plus tôt par cet autre maître du chiffrement qu'était Antoine Rossignol. Employé pour les affaires du royaume comme pour la correspondance secrète du roi, le code avait mis à mal toutes les tentatives de décryptement ennemies.

Comment se présentait le « Grand Chiffre » ? Il s'agissait d'un dictionnaire chiffré où les mots courants avaient leurs codes, les mots plus rares étant décomposés en syllabes, codées chacune de façon redondante pour éviter une analyse fréquentielle. En tout, il comportait 587 nombres. Comment Bazeries l'a-t-il cassé ? Étudiant l'ensemble des messages conservés dans les archives, il remarqua que la série « 124 22 125 46 345 » revenait souvent et émit l'hypothèse qu'elle signifiait « les–en–ne–mi–s », les ennemis. Avec cette seule supposition, le code s'écroula ensuite progressivement et Bazeries le décrypta quasi entièrement.

De façon amusante, l'une des lettres des archives déchiffrées par Bazeries offre une solution possible au mystère de l'homme au masque de fer. La lettre en question contient le passage suivant :

> « Sa Majesté vous mande d'arrêter immédiatement le général Bulonde et de le conduire à la forteresse de Pignerol pour y être écroué, gardé à vue la nuit, et autorisé à se promener sur les remparts le jour, le visage recouvert d'un 330 309 ».

Les deux nombres 330 et 309 ne se retrouvent nulle part ailleurs, si bien que Bazeries en fut réduit à supposer qu'il s'agissait d'un masque, sans doute (mal) influencé par l'énigme du masque de fer. La thèse selon laquelle le général Bulonde aurait été le prisonnier inconnu, mort à la Bastille en 1703, et connu depuis sous le nom de « masque de fer », est malgré tout difficilement défendable puisque

Bulonde, un lieutenant-général de l'armée française, était encore vivant en 1708. Cette erreur probable n'enlève rien à la valeur du décryptement de Bazeries. Son travail montre la faiblesse des codes à dictionnaires chiffrés : ils peuvent être cassés progressivement.

Les cabinets noirs

Un autre exemple historique va éclairer l'apprenti décrypteur qui sommeille en vous sur une deuxième façon de casser des codes simples. Nous allons nous glisser un instant dans la peau des membres du cabinet noir, le service de décryptement des rois de France chargé d'« écouter » les messages qui transitaient par la poste.

Réservée au courrier royal lors de sa création au XVe siècle, la poste fut rapidement mise à la disposition d'un plus large public. Pour envoyer une dépêche, l'utilisateur devait accepter la possibilité que les agents des Postes la lisent pour s'assurer qu'elle ne contenait rien d'outrageant envers le roi. La censure ne se cachait guère en cette fin du Moyen Âge. Le service de décryptement devint un cabinet noir à proprement parler avec Richelieu. Sous Louis XV, il prit le titre très officiel de *Cabinet du secret des Postes*. On y décachetait les lettres, les déchiffrait si besoin, avant de les recacheter.

Voyons comment le Cabinet noir pouvait décrypter les lettres interceptées. Pour cela, nous avons inventé un exemple plus simple que les messages réels. Tout d'abord, remarquons que la connaissance du contexte est préférable pour décrypter un message dont nous ne connaissons pas le code. Imaginons donc que nous ayons intercepté une dépêche mélangeant du clair et du chiffré – une erreur classique – et dans un contexte de guerre qui plus est. Nous savons que la dépêche est adressée au maréchal Dupont et qu'elle provient du général Durand, que nos forces viennent d'attaquer sur son flanc ouest. La voici :

> 351 – 21 – 15 – 185 – 4.51.45.66.70.85 – je suis 3061 – 25 – 4035 – 460 – 66.51.5031 – je demande deux – 405 – en – 8921.9374 – 66.51 – je m'en vais – 205 – 38 – 405 – 4.51.95.351.70.4

On y remarque des tirets et des points. La façon dont ils sont disposés invite à penser que les tirets séparent les mots et les points des lettres ou des syllabes dans les mots.

Le groupe de six chiffres « 4.51.45.66.70.85 » signifie sans doute « Dupont » et le groupe « 4.51.95.351.70.4 », Durand. La coïncidence des groupes « 4.51 » le confirme. On en déduit que les quatre nombres (351 – 21 – 15 – 185) qui précèdent « Dupont » signifient probablement « à monsieur le maréchal », puisque « 351 » signifie A. De même, ce qui précède « Durand » doit être « général de division ». Le groupe « 66.51 » et ce que nous connaissons de la situation permettent de reconstituer le message :

> À monsieur le maréchal Dupont, je suis attaqué sur mon flanc ouest, je demande deux divisions en renfort ou je m'en vais. Général de division Durand.

Du bricolage assumé

La méthode peut paraître très peu rigoureuse, puisqu'elle consiste à faire des hypothèses que seul le résultat final justifie. En fait, il s'agit de la démarche scientifique même, qui consiste à effectuer des essais et à observer leurs conséquences. La science ne progresse pas de façon déductive mais inductive, elle ne va pas du général au particulier mais l'inverse. Dans le cas du décryptement, la démarche déductive ne sert qu'ensuite à contrôler le résultat : si le message final a un sens, il est fort probable que le décryptement soit correct. N'oubliez pas non plus que, généralement, le corpus de textes ne s'arrête pas à un message. Comme dans l'affaire Dreyfus, le décrypteur disposera souvent d'autres éléments qui confirmeront ou infirmeront ses hypothèses.

Dans notre exemple, l'ennemi semble avoir facilité notre tâche par les phrases convenues du début et de la fin. Trop beau pour être vrai ? En réalité, un tel concours de

circonstances est fréquent, comme l'Histoire le montre. Nous le verrons en particulier avec les messages de l'armée napoléonienne (voir le chapitre 5). D'autre part, nous avons choisi un message court, déchiffrable rapidement. Or, en réalité, plus un message est long, plus il est facile à décrypter : il renferme alors davantage de répétitions, qui sont autant de failles dans lesquelles un décrypteur est tenté de s'engouffrer. Et même si chaque missive est courte, si le code reste identique au fil des échanges, cent messages mis bout à bout constitueront un long texte.

J'espère vous avoir convaincu que, pour toutes ces raisons, les codes figurant dans ce chapitre résistent mal à l'analyse. Pour la défense de tous les généraux ayant eu recours aux dictionnaires chiffrés, nous devons reconnaître que cette erreur traverse les âges. Ainsi, au début de la Seconde Guerre mondiale, on a cru la machine Enigma indéchiffrable à cause du nombre de possibilités de clefs différentes qu'elle offrait. Pourtant, les Polonais puis les Britanniques la décryptèrent !

Ce Qu'il Faut Décrypter

Un chiffre pour Othon

Le message chiffré suivant est visiblement destiné à Othon Carsonfuhi :

405 125 236 052 341 503 325 052 125 341 405 325 503 325 236

Saurez-vous le décrypter ?

Les messages personnels de la BBC

Pour finir sur les dictionnaires chiffrés, impossible de ne pas évoquer les fameux messages personnels de la BBC pendant la Seconde Guerre mondiale. Après l'appel du 18 juin lancé sur les ondes par le général de Gaulle, une émission quotidienne fut créée pour s'adresser directement aux Français. Inaugurée sous le nom de « Ici la France » le 14 juillet 1940, elle devint bientôt « Les Français parlent aux Français ». Son célèbre indicatif au son de percussions, « POM-POM-POM-POOOM », pouvait aussi bien être entendu comme le début stylisé de la V^{e} symphonie de Beethoven que comme le « V » de la victoire en code Morse : • • • — (trois POM courts et un POM long).

Outre des nouvelles de la guerre, expurgées de la propagande allemande, cette émission diffusait des messages personnels destinés pour l'essentiel à des réseaux de résistance. Les phrases poétiques ou amusantes cachaient des préparations de parachutages d'hommes ou d'armes, l'organisation d'opérations de guérilla, etc.

Les sanglots longs des violons de l'automne bercent mon cœur d'une langueur monotone	Saboter les voies ferrées (en préparation du débarquement du 6 juin 1944)
C'est évidemment un tort	Faites donner immédiatement vos sections antichars
Écoute mon cœur qui pleure	Opération d'atterrissage du 15 juin 1943

Frédéric était roi de Prusse. Nous disons quatre fois.	Parachutage (4 avions)
Gabrielle vous envoie ses amitiés	Parachutage à réceptionner (20 octobre 1941)
Il a pleuré de joie	Parachutage d'armes et d'agents
Il a une voix de fausset	Déclenchement de la guérilla
Il est sévère mais juste (plus code du département)	Commencer les sabotages la nuit même
Il fait chaud à Suez	Déclenchement du plan vert, à Paris
Je n'aime pas la blanquette de veau	Parachutages vers Donnemarie-Dontilly
Jean a une moustache très longue	Faire sauter les lignes de communication entre la zone de débarquement et les QG allemands
L'acide rougit le rossignol	Message actions guérillas ; sans exception, les hommes devront entrer en lice, la grande aventure commencera
L'angora a les poils longs	Parachutage d'armes
L'heure des combats viendra	Annonce le débarquement et constitue l'ordre de lancement des opérations de sabotages des voies ferrées de l'ouest
Ma femme a l'œil vif	Ne pas bouger
Messieurs, faites vos jeux	Ordre de sabotages (nuit du 5 juin)

Quelques messages de la BBC avec leur signification.

Remarquez que, dans le premier message, contrairement à la légende, il ne s'agit pas du poème de Verlaine (voir page suivante) car, dans celui-ci, les sanglots blessent, ils ne bercent pas. En fait, le texte fait référence à la chanson de Charles Trenet. Sans connaître son sens, les Allemands auraient pu comprendre que les Alliés débarqueraient vers le début du mois de juin 1944, tout simplement en

constatant l'augmentation du nombre de messages les semaines précédentes. Ce nombre culmina à 200 le 5 juin ! Destinés à un usage unique, ces messages n'étaient pas codés. Il s'agissait simplement de phrases types qui permettaient de transmettre un signal d'action à la Résistance. Même le plus malin et mathématicien des cryptologues n'aurait pas su les décrypter.

Les codes télépathiques

Pour clore ce chapitre, je vous propose de quitter un peu le monde des intrigues militaires ou politiques et de finir de façon plus légère, avec l'application des codes secrets sur l'estrade des cabarets. Place aux artistes de music-hall et à leur pseudo-don de télépathie ! Pour se mettre dans l'ambiance, le mieux est encore de se rappeler le sketch hilarant de Pierre Dac et Francis Blanche, *Le sâr Rabindranath Duval* (1957), devenu culte :

– Votre Sérénité, pouvez-vous me dire, c'est très important, concentrez-vous, pouvez-vous me dire quel est le numéro du compte en banque de monsieur ?
– Oui.
– Vous pouvez le dire ?
– Oui !!
– Vous pouvez le dire ?
– Oui !!
– Il peut le dire !!! Bravo ! Il est extraordinaire, il est vraiment sensationnel.

Ce sketch était inspiré par la performance d'un couple d'artistes, Myr et Myroska, qui s'était rendu célèbre grâce à un tour de « magie » *a priori* à haut risque. Myroska restait sur scène, les yeux bandés, tandis que Myr descendait dans la salle. Le public lui présentait des objets variés, carte d'identité, portefeuille, etc. Invariablement, Myroska devinait ce que Myr avait dans les mains. Dans une de ses prestations, elle affirma effectivement, à propos d'un numéro de compte en banque : « Je peux le dire », comme

Pierre Dac plus tard. La différence est qu'elle donna les quatre derniers chiffres. Ils se révélèrent tous exacts.

Sauf à croire à la transmission de pensée, il faut bien imaginer un moyen physique en jeu. Plusieurs hypothèses ont été émises, dont l'utilisation de communications radio, mais il semble que le système télépathique de Myr et Myroska reposait plutôt sur un code. Par exemple, Myr répétait souvent de manières différentes : « Myroska, êtes-vous avec moi ? » Cela suffisait-il à Myr pour transmettre les renseignements à Myroska ? Difficile de l'affirmer. Il est possible que le message était distribué dans ses autres phrases, ses pauses, etc.

Myr et Myroska utilisaient-ils un code secret dans leur spectacle de « télépathie » ?

De nombreux artistes ont repris le flambeau avec succès, sans que personne ne réussisse jamais à trouver le système de Myr et Myroska. Cette idée n'enlève rien à la

performance car, même si le code ne comporte que quelques centaines de symboles, comme le Grand Chiffre de Louis XIV, il est nécessaire que les deux artistes l'aient en tête, le mobilisent très rapidement et de façon naturelle. Comme le disait Myr à la fin de chacun de ses numéros :

> S'il n'y a pas de truc, c'est formidable, mais s'il y a un truc, reconnaissez que c'est encore plus formidable.

Ce serait extraordinaire, donc encore plus formidable, de découvrir leur truc sans retrouver le petit livre dans lequel ils l'avaient certainement consigné. Nul doute que cette tâche réclamerait les cellules grises d'un cryptanalyste de bon niveau, condamné à visionner un grand nombre de leurs spectacles. Mais à quoi bon désenchanter notre monde, qui ne l'est déjà que trop ?

Une recette pour la télépathie

Vous souhaitez vous aussi vous prendre pour Myr et Myroska et échanger des messages sans que votre entourage ne s'en aperçoive ? Pour cela, convenez d'un code entre votre partenaire et vous. Voici une idée volontairement très simple.

Une phrase commençant par « je » signifie « 1 », une phrase commençant par « tu » signifie « 2 », une phrase commençant par « il » signifie « 3 », de même « nous » pour « 4 », « vous » pour « 5 ». Comment poursuivre ? Retenez un mot – ou plusieurs pour mieux tromper l'ennemi – à ajouter dans la phrase pour obtenir dans l'ordre « 6 », « 7 », « 8 » et « 9 ». Si ce mot est « mais », et que vous voulez transmettre mentalement 283 à votre complice, il suffira de dire, par exemple : « Tu es avec moi Sophie ? ». Quoi qu'elle réponde, vous poursuivrez :

« Il fait froid, mais je continue », puis : « Il fait vraiment froid. »

Si Sophie a compris le code, elle saura que le nombre caché est 283. Une question reste : comment transmettre 0 ? La règle la plus simple est de convenir que toute phrase sortant du cadre précédent signifie 0. Bien sûr, si le sujet vous intéresse, vous trouverez des codes plus raffinés et permettant de transmettre bien plus de pensées qu'un simple nombre. À vous de créer le vôtre !

Ce Qu'il Faut Décrypter

Transmission de pensée

Un nombre est caché derrière cette suite de phrases :

« Il fait beau mais froid »
« Tu ne trouves pas »
« Oui »
« Vous pensez pareil ? »

Saurez-vous le trouver ?

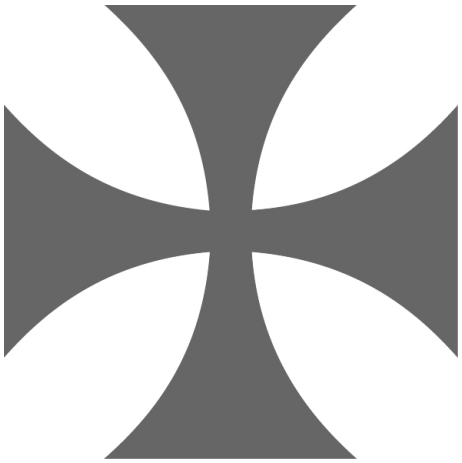
3 Les codes des initiés

Les militaires et les rois (mais aussi les télépathes, voir le chapitre précédent) n'ont pas été les seuls adeptes de la science cryptographique au long de l'Histoire. Une autre catégorie de personnes a éprouvé le besoin de dissimuler leurs communications : les sociétés secrètes. Frappées du sceau de l'interdit, certaines avaient un besoin vital de cacher des informations vis-à-vis du pouvoir ou de l'Église, mais ce n'était pas l'unique raison qui les poussait à chiffrer leurs échanges.

En fait, un grand nombre de codes historiques, comme ceux des Templiers ou des francs-maçons, étaient liés à une initiation, à l'utilisation de symboles étranges (que l'on qualifierait de cabalistiques si ce mot n'avait pas un sens précis, lié à la Cabale) qui liaient leurs utilisateurs et leur conféraient un sentiment d'appartenance non seulement à un groupe, mais à une élite.

Ces codes des *initiés* semblent *a priori* indéchiffrables sans connaître leur principe. En réalité, il existe une méthode systématique permettant de les briser. Inconditionnels du *Da Vinci Code*, ce chapitre est pour vous !

L'énigme des Templiers



La croix des Templiers ornait leurs boucliers. De façon plus secrète, leur chiffre était fondé sur cette croix.

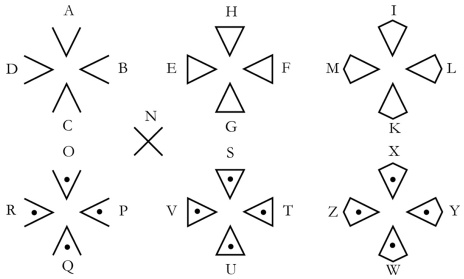
Laquelle de ces sociétés secrètes est-elle la plus connue des adolescents d'aujourd'hui ? Sans nul doute l'ordre des Templiers. C'est en effet l'une des deux confréries qui se livrent bataille dans le jeu vidéo à succès *Assassin's Creed*… L'ordre du Temple a été fondé en 1129 dans le contexte des croisades. Il regroupait au départ des moines-soldats chargés d'aller défendre la Terre sainte. Sa puissance financière, autant que militaire, finit par éveiller la jalousie et l'inquiétude des rois de France, puis l'ordre fut dissous par le pape en 1312 à la suite d'un procès en hérésie. Ses principaux dignitaires, dont le maître de l'ordre, Jacques de Molay, furent brûlés vifs sur l'île de la Cité, à Paris. D'après un chroniqueur de l'époque, les dernières paroles du maître furent :

> Dieu sait qui a tort et a péché, et le malheur s'abattra bientôt sur ceux qui nous condamnent à tort. Dieu vengera notre mort. Seigneur, sachez que, en vérité, tous ceux qui nous sont contraires, par nous auront à souffrir.

Effectivement, le malheur s'abattit : le pape comme le roi moururent peu après le procès, et l'hécatombe continua les années suivantes parmi leurs comparses. Cette série de coïncidences alimenta de nombreux mythes greffés par la suite sur la réalité historique, tel le fameux trésor que les Templiers auraient caché avant la dissolution de l'ordre et que certains s'évertuent encore à chercher aujourd'hui.

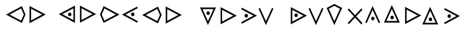
Si vous faites partie de ces infatigables prospecteurs à la poêle à frire, si vous voulez retrouver le trésor de pirates comme Olivier Levasseur, dit la Buse, qui a écumé l'océan indien au XVIIIe siècle,

la suite va vous intéresser. Je ne cite pas Levasseur par hasard, car son nom est bel et bien lié à un cryptogramme et à un trésor. Le jour où il fut pendu sur l'île de la Réunion, il jeta un papier à la foule venue assister à son exécution en criant : « Mon trésor à qui saura comprendre ! » Je ne vous donnerai pas le cryptogramme figurant sur ce papier, car il en existe plusieurs versions dont l'authenticité est impossible à vérifier, mais je vais vous donner la clef pour le décrypter car il est de même nature que ceux des Templiers et des francs-maçons (que nous voyons plus loin). Commençons donc par le chiffre que les Templiers employaient pour communiquer. Il est facile à retenir car fondé sur la croix.



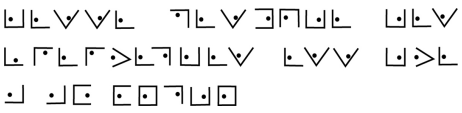
Dans le chiffre des Templiers, chaque lettre (sauf le J, que l'on confond avec le I) est remplacée par un symbole. Ce type de chiffre est appelé « chiffre par substitution alphabétique » car chaque lettre y est substituée par un autre symbole.

Ainsi pour chiffrer : « le Temple sera vainqueur », nous écrirons :



Cette écriture paraît indéchiffrable à cause de l'étrangeté des lettres. En fait, ce code est facile à casser, comme nous allons le voir via un petit détour par un chiffre du même type, puisque nous avons donné le secret de celui des Templiers.

Imaginons que nous ayons intercepté l'étrange message suivant :



Comment le déchiffrer ? Un examen rapide laisse penser à une substitution de notre alphabet latin habituel par un autre, le découpage des mots ayant été vraisemblablement conservé. L'idée pour trouver le sens de chaque symbole remonte à un savant arabe, Abu Yusuf Al-Kindi (801-873), qui constata que, dans deux textes assez longs, les fréquences d'apparition de chaque lettre étaient proches. Cette propriété se retrouve dans toute langue écrite au moyen d'un alphabet. Voici comment il décrit lui-même sa méthode dans son *Manuscrit sur le déchiffrement des messages cryptographiques* :

> Une façon d'élucider un message chiffré, si nous savons dans quelle langue il est écrit, est de nous procurer un autre texte clair dans la même langue, de la longueur d'un feuillet environ, et de compter alors les apparitions de chaque lettre. Nous appellerons la lettre apparaissant le plus souvent la « première », la suivante la « deuxième », et ainsi de suite pour chaque lettre figurant dans le texte. Ensuite, nous nous reportons au texte chiffré que nous voulons éclaircir et nous relevons de même les symboles. Nous remplaçons le symbole le plus fréquent par la lettre « première » du texte clair, le suivant par la lettre « deuxième », le suivant par la « troisième », et ainsi de suite jusqu'à ce que nous soyons venus à bout de tous les symboles du cryptogramme à résoudre.

Un saint à la rescousse

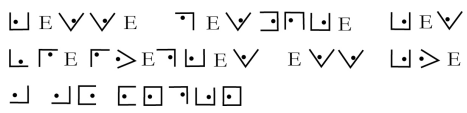
Ainsi, en calculant les fréquences d'apparition de chaque symbole dans un texte chiffré comme ci-dessus et en les comparant aux fréquences usuelles, il est possible de retrouver les substitutions mobilisées.

A	B	C	D	E	F	G	H	I	J	K	L	M
8,4	**1,1**	**3,0**	**4,2**	**17,3**	**1,1**	**1,3**	**0,9**	**7,3**	**0,3**	**0,1**	**6,0**	**3,0**
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
7,1	**5,3**	**3,0**	**1,0**	**6,5**	**8,1**	**7,1**	**5,7**	**1,3**	**0,1**	**0,4**	**0,3**	**0,1**

Tableau de fréquences des lettres en français, exprimées en pourcentages. Le E est la lettre la plus fréquente.

Une méthode mnémotechnique pour retenir les lettres les plus fréquentes en français est de penser que saint Urlo est le saint patron des cryptologues, ce qui apparaissait dans de vieux chants militaires aujourd'hui oubliés (n'allez pas croire que saint Urlo, en raison de son patronyme bizarre, est imaginaire, il s'agit d'un saint breton). En effet, après le E, les lettres les plus fréquentes sont celles de l'expression « saint Urlo ». À elles seules, ces dix lettres composent 80 % du contenu des textes en français moderne. On verra plus loin comment exploiter cette propriété pour décrypter un texte chiffré, même lorsqu'il est issu du roman *La Disparition*, pourtant rédigé sans la lettre E !

Dans le cas du message précédent, le même symbole ⌊• (en deuxième position) apparaît 10 fois sur 39 : il représente manifestement E. En le remplaçant par cette lettre dans le message, on obtient :

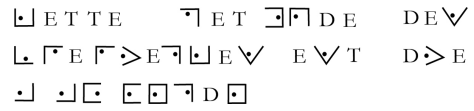


Première étape du décryptement. Les mots commencent à se former, les espaces entre eux sont une aide.

Après ⌊•, les symboles les plus fréquents sont ⩗ et ⌊• (en troisième et onzième positions). Ils sont représentés quatre fois. La position redoublée du premier et encadrée par deux E implique qu'il s'agit d'une consonne. Les candidats vraisemblables sont N, R, S et T, mais le redoublement et la taille du mot milite pour T. Essayons donc cette éventualité. La position du deuxième dans un mot de trois lettres devant la voyelle E suggère également une consonne, L, M ou D, puisque T est à exclure dans notre hypothèse.

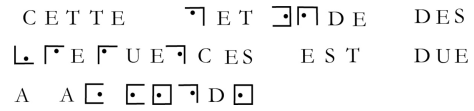
Avant d'aller plus loin, arrêtons-nous un instant sur ce qui peut sembler un manque de rigueur. Comme nous l'avons déjà vu avec l'exemple d'Étienne Bazeries, sélectionner une hypothèse parmi

plusieurs possibles est courant chez les décrypteurs. Seul le résultat final nous dira si nous avons eu raison ou non de l'envisager. Le décryptement des textes passe souvent par des essais de ce type. Cependant, nous ne rapportons pas nos éventuels essais infructueux car la règle est simple : quand nous parvenons à une impossibilité, nous rebroussons chemin. En essayant T et D, nous obtenons dès lors :



Deuxième étape du décryptement.

La décomposition du message en mots est une aide. Un jeu de devinettes permet de trouver la valeur de quelques symboles. Par exemple, le premier mot est sûrement « cette », le dernier de la première ligne « des » et les deux derniers de la seconde « est due ». Enfin, le symbole isolé est probablement A. Nous avons donc :



Troisième étape du décryptement.

Parvenu à ce point, la solution est question d'imagination, la phrase étant trop courte pour déployer la méthode des fréquences sur des lettres peu usuelles. Ici, il est malgré tout facile de combler la suite. Le message signifie :

« Cette méthode des fréquences est due à Al-Kindi ».

Ce petit exemple, que nous avons forgé, montre qu'il suffit de posséder quelques phrases codées par ce genre de chiffre pour le décrypter.

Message d'un cryptologue

Un mathématicien vous envoie le message :

& EJHH R D& O&& %RJDS & R

Dans l'hypothèse où vous savez que l'expéditeur y parle de chiffres, cette information vous suffira-t-elle pour le décrypter ?

Le plus célèbre

Ce chapitre regroupe certains codes qui n'ont jamais servi sur des théâtres de guerre. Curieusement, le chiffre plus utilisé dans l'Histoire appartient à cette catégorie de codes « pacifistes ». À votre avis, de quel code s'agit-il ? Un indice : à tous les coups, vous savez coder l'expression SOS. Je veux bien sûr parler du morse. La présence du morse dans ces pages pourrait paraître incongrue, puisque ce n'est pas un chiffre destiné à cacher le sens de messages, mais après tout il s'agit d'un code comme un autre.

De nos jours, le code morse semble n'avoir plus qu'un intérêt historique, quoique certaines parties du spectre radio lui restent réservées. Pourquoi ? Tout simplement parce qu'il demande moins d'équipement que d'autres formes de communications radio et reste exploitable avec un bruit de fond important et un signal faible. Il a été inventé par Samuel Morse (1791-1872) afin de transmettre des messages au moyen de signaux électriques ou optiques. Il utilise deux signaux : un long et un bref, notés par un tiret court et un tiret long. Le plus long vaut trois fois le plus petit et, dans une même lettre, chaque signal est séparé du suivant par un silence de la longueur d'un signal bref. Ainsi, le signal le plus bref (le point, noté •) vaut 1 unité de temps arbitraire (comme une noire peut valoir 1 temps en musique), le plus long (le trait, noté —) vaut 3 et deux brefs suivis d'un long vaut 5.

Le choix du code a été fait en tenant compte de ces longueurs : les caractères les plus fréquents en anglais sont codés par les signaux les plus courts. Ainsi, la voyelle E, dont la fréquence est de 12,56 % en anglais, correspond au signal le plus bref (•). Ensuite vient la lettre T dont la fréquence est de 9,15 % (—). Le

code s’explique assez bien en construisant la table des codes possibles selon leur longueur. Pour que ce tableau reste lisible, nous nous limitons aux lettres de l’alphabet.

1	• E 12 %
3	• • I 7 % — T 9 %
5	• • • S 7 % • — A 7 % — • N 7 %
7	• • • • H 5 % • • — U 3 % • — • R 6 % — • • D 4 % — — M 3 %
9	• • • — V 1 % • • — • F 2 % • — • • L 4 % — • • • B 2 % • — — W 2 % — • — K 1 % — — • G 2 %
11	— • — • C 3 % • — — • P 2 % — • • — X 0,2 % — — • • Z 0,1 %
13	• — — — J 0,1 % — — • — Q 0,1 % — • — — Y 2 %

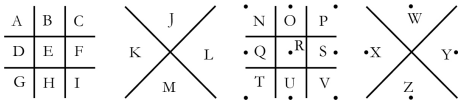
Les codes selon leur longueur. Les lettres les plus fréquentes en anglais se trouvent toutes dans les trois premières lignes. On trouve quelques rares anomalies ensuite (C, L et Y).

L’écriture secrète des francs-maçons

Mais revenons aux codes secrets – ou, en tout cas, à ceux qu’on a cru être secrets ! Un chapitre sur les codes des initiés ne saurait faire l’impasse sur la confrérie la plus soupçonnée d’entretenir des liens avec l’occulte et le secret : les francs-maçons. Les *frères* ont communiqué entre eux à l’aide d’un chiffre simple, aussi

rudimentaire que celui des Templiers, jusqu'au XIXe siècle ! Quelques phrases écrites dans ce chiffre suffisaient pourtant à le casser. Il est étonnant que la confrérie en ait pris conscience si tardivement, alors même que la méthode des fréquences datait du IXe siècle. La raison est sans doute qu'il est rare de voir les briseurs de codes se vanter de leurs exploits (en outre, les espions ne laissent guère leurs empreintes digitales sur l'objet de leur forfait) et, comme nous l'avons vu avec le chevalier de Rohan, les vantards sont rarement les vrais décrypteurs.

Les francs-maçons nommaient leur code si peu secret Pig-Pen, l'« enclos aux porcs » en anglais. Il se fondait sur des figures géométriques simples, des grilles à l'apparence de parcs à cochons, d'où son nom qui était évidemment aussi un clin d'œil à Big Ben, la grande cloche du palais de Westminster. Comme celui des Templiers, ce chiffre avait l'avantage d'être facile à retenir.



Chiffre des francs-maçons, dit Pig-Pen.

Ce Qu'il Faut Décrypter

Un message maçonnique

Voici un message maçonnique :

Saurez-vous y voir clair ?

Les diverses archives, comme celles de la ville de Strasbourg – j'ai eu un accès privilégié, à des fins d'expertise, à son riche fonds de documents chiffrés –, contiennent des chiffres un peu plus élaborés quoique du même type, où la graphie rappelle les chiffres des Templiers et des francs-maçons. Celui que nous présentons ci-

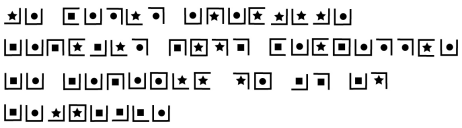
dessous date de 1627 : il concerne le procès en sorcellerie de Séraphin Hénot (eh oui, pour bâtir une défense en justice, le secret peut être nécessaire), secrétaire intime de l'archiduc Léopold d'Autriche, évêque de Strasbourg. Comme vous pouvez le constater vous-mêmes, outre les lettres de l'alphabet, le chiffre prévoit aussi le codage de certains digrammes, comme FF, et de certains mots ou noms courants (dont l'ensemble constitue ce qu'on nomme un nomenclateur, voir ci-dessous). Ajouter ces signes améliore la solidité de ce type de chiffre, mais ne le rend pas pour autant incassable, loin de là. Ces chiffres « améliorés » restent encore très faibles, comme nous le verrons plus loin.

Le chiffre de l'affaire Hénot daté de 1627 et conservé aux archives de Strasbourg : une substitution alphabétique simple, avec chiffrement de digrammes et nomenclateur (les deux lignes du bas).

L'avantage du chiffre des francs-maçons est que le déchiffrement d'un message est facile. L'ennui, c'est que le casser est à peine plus compliqué ! Nous avons créé un chiffre du même type pour vous en convaincre, les points étant remplacés par des carrés, des ronds et des étoiles (voir ci-dessous *Un message pour vous*). Bien entendu, le travail demande quand même du temps et des calculs pour appliquer la méthode des fréquences !

Un message pour vous

Voici un message écrit par une méthode digne des francs-maçons :



À vous de le décrypter !

Le mystère du scarabée d'or

Une île couverte d'épaisses broussailles, un vieux parchemin écrit à l'encre invisible, un trésor enfoui : tous les ingrédients d'une bonne vieille histoire de pirates fleurant bon le rhum sont réunis dans la nouvelle *Le Scarabée d'or* d'Edgar Allan Poe. Avec en prime, un code à déchiffrer ! Pourquoi citer Edgar Poe ici ? C'est que, grâce à sa nouvelle, il contribua grandement à populariser les codes secrets au milieu du XIXe siècle et à répandre leur aura de mystère. Il faut dire que Poe (1809-1849) maîtrisait à la perfection l'art de décrypter les chiffres comme ceux des chapitres précédents, sans doute un héritage de ses études à West Point, l'académie militaire américaine.

Alors qu'il collaborait à un journal de Philadelphie, l'*Alexander's Weekly Messenger*, il lança un défi aux lecteurs, affirmant qu'il serait capable de décrypter tous les textes chiffrés ! Des centaines de lecteurs envoyèrent des cryptogrammes et les seuls qu'il ne décrypta pas semblent bien avoir été des lettres simplement disposées au hasard. Il expliqua ensuite sa méthode dans *Le Scarabée d'or*. Elle consiste en un mélange d'analyse des fréquences et de recherche de mots probables. Voici le message secret de la nouvelle :

53‡‡†305))6*;4826)4‡.)4‡);806*;48†8
¶60))85;1‡(;:‡*8†83(88)5*†;46(;88*96
?;8)‡(;485);5*†2:*‡(;4956*2(5*—4)8
¶8*;4069285);)6†8)4‡‡;1(‡9;48081;8:8‡
1;48†85;4)485†528806*81(‡9;48;(88;4
(‡?34;48)4‡;161;:188;‡?;

Ce message contient 20 symboles différents, dont le héros calcule d'abord les fréquences pour les comparer aux fréquences moyennes en anglais.

	;		‡	)	*			(	†
8		**4**				**5**	**6**		
16,3	**12,8**	**9,4**	**7,9**	**7,9**	**6,4**	**5,9**	**5,4**	**4,9**	**3,9**
1	**0**	**2**	**9**	**3**	:	?	¶		—
3,9	**3,0**	**2,5**	**2,5**	**2,0**	**2,0**	**1,5**	**1,0**	**0,5**	**0,5**

Fréquences des symboles dans le texte.

A	B	C	D	E	F	G	H	I	J	K	L	M
8,1	**1,7**	**3,2**	**4,0**	**12,6**	**2,2**	**1,8**	**5,3**	**7,2**	**0,1**	**0,6**	**4,0**	**2,6**

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
7,4	**7,5**	**1,9**	**0,1**	**6,4**	**6,6**	**9,1**	**2,8**	**1,0**	**1,9**	**0,2**	**1,6**	**0,1**

Fréquences des lettres en anglais.

Cette comparaison n’est concluante que pour la lettre la plus fréquente, E (8). Le personnage de Poe exploite alors la méthode du mot probable, en remarquant que le mot anglais le plus utilisé est l’article « THE ». Il cherche donc des répétitions de trois symboles finissant par 8. Il trouve la suite de trois symboles « ;48 » sept fois :

53‡‡†305))6***;48**26)4‡.)4‡);806***;48**†8
¶60))85;1‡(;:‡*8†83(88)5*†;46(;88*96
?;8)‡(**;48**5);5*†2:*‡(;4956*2(5*—4)8
¶8*;4069285);)6†8)4‡‡;1(‡9**;48**081;8:8‡
1**;48**†85;4)485†528806*81(‡9**;48**;(88;4

(‡?34**;48**)4‡;161;:188;‡?;

Le décryptement proprement dit peut ensuite commencer :

53‡‡†305))6*THE26)H‡.)H‡)TE06*THE†E
¶60))E5T 1‡(T:‡*E†E3(EE)5*†TH6(TEE*96
?TE)‡(THE5)T 5*†2:*‡(TH956*2(5*—H) E
¶E*TH0692E5)T)6†E)H‡‡T1(‡9THE0E1TE: E‡
1THE†E5TH)HE5†52EE06*81(‡9THET(EETH
(‡?3HTHE)H‡ T161T:1EET‡?T

Le héros s'attaque alors aux séquences dont la majorité des lettres sont connues, comme « **THET**(**EETH** ». Quelques essais lui montrent alors que le symbole « (» désigne la lettre « R ». Le message se précise, ce qui l'amène à réaliser d'autres tentatives et ainsi de suite. Finalement, il aboutit à la solution :

> A good glass in the bishop's hostel in the devil's seat forty-one degrees and thirteen minutes northeast and by north main branch seventh limb east side shoot from the left eye of the death's-head a bee line from the tree through the shot fifty feet out.

Soit, dans la traduction française du texte :

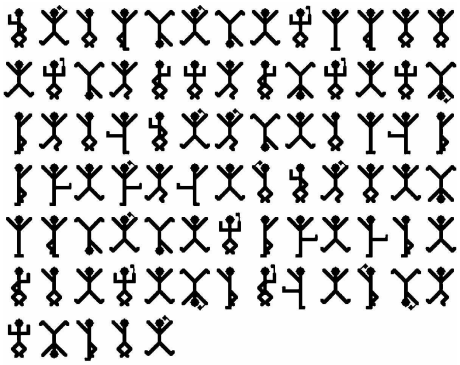
> Un bon verre dans l'hôtel de l'évêque dans la chaise du diable quarante et un degrés et treize minutes nord-est quart de nord principale tige septième branche côté est lâchez de l'œil gauche de la tête de mort une ligne d'abeille de l'arbre à travers la balle cinquante pieds au large.

Nous retrouverons souvent chez les cryptologues cette méthode associant calculs mathématiques et conjectures linguistiques. Dans *Les Hommes dansants* de Conan Doyle, Sherlock Holmes a recours à la même technique pour décrypter un message codé par substitution alphabétique, sachant que le détective dispose en plus d'un indice : un petit drapeau marquant la fin de chaque mot. Dans ce cas, la substitution a en outre une vertu stéganographique. En regardant le message codé, on pourrait croire de prime abord (comme le docteur Watson dans la nouvelle) à des dessins d'enfants.

Ce Qu'il Faut Décrypter

Les hommes dansants

Voici un message écrit avec le code des hommes dansants de Conan Doyle :



Que signifie-t-il ?

Parmi les écrivains s'étant intéressés à la cryptographie, citons également Jules Verne, qui usa dans ses textes de méthodes plus élaborées, comme le montre le chapitre 8 sur les substitutions poly-alphabétiques et le chapitre 6 sur les chiffres par transposition.

Acrostiches et autres fantaisies cryptiques

Comme les romanciers, les poètes ont aussi cherché à dissimuler des messages à l'intérieur de leurs œuvres. S'ils n'ont pas manipulé des codes secrets à proprement dit, leur démarche s'en inspire (en fait, elle ressemble plus directement à la technique de stéganographie). Regardez, par exemple, comme ce fameux pamphlet datant de la Seconde Guerre mondiale s'amuse à cacher sa véritable intention, derrière des louanges adressées à Hitler.

Aimons et admirons
L'éternelle Angleterre
Maudissons, écrasons
Le nazi sur la terre
Soyons donc le soutien
De ces navigateurs
À eux seuls appartient
La palme du vainqueur

le chancelier Hitler
est indigne de vivre
le peuple d'outre-mer
sera seul à survivre.
du Führer allemand
la race soit maudite.
ce juste châtiment
répond au vrai mérite.

La lecture ligne par ligne donne un message collaborationniste, « Aimons et admirons le chancelier Hitler ! » et colonne par colonne un soutien à la Couronne britannique, « Aimons et admirons l'éternelle Angleterre. »

Pour délivrer un message, les poètes ont aussi pratiqué l'acrostiche, un type de poème où les premières lettres de chaque vers peuvent être lues verticalement. Le plus célèbre acrostiche est de Pierre Corneille, dans *Horace* :

S'attacher au combat contre un autre soi-même,
Attaquer un parti qui prend pour défenseur
Le frère d'une femme et l'amant d'une sœur,
Et rompant tous ces nœuds, s'armer pour la patrie
Contre un sang qu'on voudrait racheter de sa vie,
Une telle vertu n'appartenait qu'à nous ;
L'éclat de son grand nom lui fait peu de jaloux,

La présence de ce « sale cul » en tête de vers est difficile à attribuer au hasard, d'autant plus qu'il revêt un sens dans le contexte du poème, l'attitude d'Horace y étant inhumaine. Son pendant le plus comique est sans doute dû à Henry Gauthier-Villars, dit Willy, ce journaliste, critique musical et romancier qui fut le premier mari de Colette. Après avoir eu maille à partir avec un directeur de journal genevois nommé Charles Hubacher (son identité a de l'importance), qui l'avait traité de « dévoyé du Moulin-Rouge », Willy prit sa revanche en envoyant sous pseudonyme le sonnet suivant à un journal pacifiste français, qui le publia aussitôt. Sans prendre la peine de demander l'autorisation de l'auteur, Hubacher le reproduisit dans son journal, tombant sans le savoir dans le piège que lui tendait le journaliste.

Hélas ! À chaque instant, le mal terrible empire !
Un cyclone de haine et de férocité
Bouleverse les champs, ravage la cité,
À flots coule le sang sous les dents du vampire.
Cruauté d'autrefois ! Cet ancestral délire,
Honnis soient les bandits qui l'ont ressuscité,
Et honte à ceux dont la cruelle surdité
Refuse d'écouter la pacifique lyre.
C'est assez de combats, de furie et de deuil,
Rien ne demeurera si nul ne s'interpose
Entre les ennemis qu'enivre un même orgueil.
Toute raison à la Raison est-elle close ?
Impuissante, se peut-il que sur l'âpre écueil,
Nous laissions se briser notre nef grandiose ?

Charles Hubacher venait de publier un poème dont les initiales formaient le message : « Hubacher, crétin ! »… Sans s'être inquiété de la véritable identité de l'auteur, il apportait la preuve même de cette affirmation. Pour finir sur le sujet des acrostiches, en voici un adapté au sujet de ce livre.

Hackers, décodeurs, décrypteurs,
Espions, anonymes masqués,
Redoutables chapardeurs,
Voilés d'opaques étiquettes,
Énigmatiques, et quantiques, vos réseaux
Libèrent aussi les mauvais chiffres
Égarent les sots et même les oiseaux.
Hachant à coups de griffes
Nombres, pétroglyphes et argots
Isolant au cœur le message
Nébuleuse d'asymétriques codages
Génie acquis ou vieil héritage ?

Petit détour par la bande dessinée : Hergé utilise un procédé comparable dans *Le Lotus bleu*. Tintin y capte par radio le message *a priori* incompréhensible suivant :

entre voie yokohama ns maison r charles andre dimanche seul aligner écran ou tentures serpent marchera inévitablement e proche occident halte intrus e

Tintin finit par trouver la clef pour décrypter ce message : il suffit de prendre les deux premières lettres de chaque mot. Ce faisant, il obtint : « Envoyons marchandise à l'écoute semaine prochaine. » Bien entendu, il est facile d'imaginer un grand nombre de codes de ce type… aussi fragiles les uns que les autres.

Ce Qu'il Faut Décrypter

Tintinophilie

Voici un message digne de Tintin :

De Charles Ifrah,
Fraîchement éreinté, espère tube NTM, rare valeur illusoire.
La bonté rieuse euphorique. X.

Saurez-vous le décrypter ?

Les codes des amoureux

Il est difficile de conclure le sujet sans citer le célèbre poème attribué à George Sand et destiné à Alfred de Musset. En fait, il s'agirait d'un canular de la fin du XIX^e^ siècle, mais cela n'enlève rien à la performance.

Cher ami,
Je suis très émue de vous dire que j'ai
bien compris l'autre soir que vous aviez
toujours une envie folle de me faire
danser. Je garde le souvenir de votre
baiser et je voudrais bien que ce soit
une preuve que je puisse être aimée
par vous. Je suis prête à vous montrer mon
affection toute désintéressée et sans cal-
cul, et si vous voulez me voir ainsi
vous dévoiler sans artifice mon âme
toute nue, venez me faire visite.
Nous causerons et en amis, franchement,
je vous prouverai que je suis la femme
sincère, capable de vous offrir l'affection
la plus profonde comme la plus étroite
amitié, en un mot la meilleure épouse
dont vous puissiez rêver, puisque votre
âme est libre. Pensez que l'abandon où je
vis est bien long, bien dur et souvent bien
insupportable. Mon chagrin est trop
gros. Accourrez bien vite et venez me le
faire oublier. À vous je veux me sou-
mettre entièrement.
Votre poupée.

La lettre romantique devient d'une tout autre nature si on ne lit qu'une ligne sur deux. Bien entendu, le canular ne s'arrête pas là, la réponse d'Alfred de Musset est tout aussi intéressante, d'autant qu'il précise lui-même comment la déchiffrer.

Quand je mets à vos pieds un éternel hommage,
Voulez-vous qu'un instant je change de visage ?
Vous avez capturé les sentiments d'un cœur
Que pour vous adorer forma le Créateur.
Je vous chéris, amour, et ma plume en délire
Couche sur le papier ce que je n'ose dire.
Avec soin, de mes vers lisez les premiers mots
Vous saurez quel remède apporter à mes maux.

Alfred de Musset

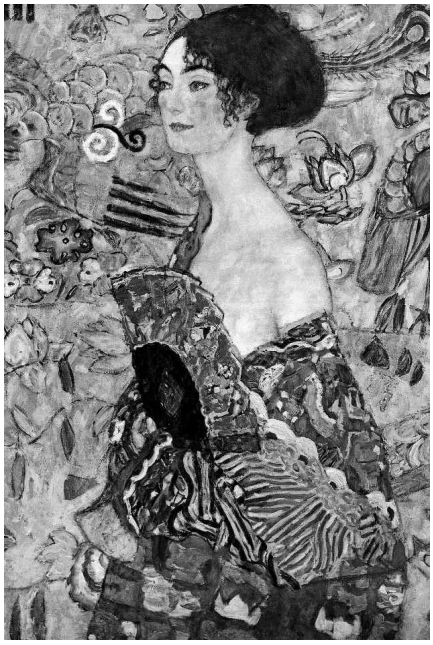
La réponse de George Sand est courte et utilise la règle donnée par Musset :

Cette insigne faveur que votre cour réclame
Nuit à ma renommée et répugne à mon âme.

George Sand

Le code des éventails

Des codes secrets peuvent aussi devenir un moyen de communication dans le monde physique. À l'époque où les jeunes filles de la cour d'Espagne étaient très surveillées, elles inventèrent un code fondé sur la position et les mouvements de leurs éventails, appelés de la sorte à devenir des instruments de séduction. Placer un éventail près du cœur signifiait ainsi « Tu as gagné mon amour », tandis que le placer sur les lèvres indiquait « Embrasse-moi »…



Dame avec un éventail, Gustav Klimt (1862-1918). Sa façon de tenir son éventail signifie « Tu as gagné mon amour ». L'histoire ne dit pas si Klimt l'a placé ainsi volontairement.

S'éventer lentement	Je suis mariée
… rapidement	Je suis fiancée
Laisser l'éventail reposer sur sa joue droite	Oui
… sur sa joue gauche	Non

Maintenir l’éventail sur l’oreille gauche	Laissez-moi tranquille
Tournoyer l’éventail avec la main droite	J’en aime un autre
… avec la main gauche	Nous sommes surveillés
Toucher avec le doigt sa partie haute	Je voudrais te parler
Descendre l’éventail, le laisser pendre	Nous serons amis
Le placer devant le visage en main gauche	À quoi penses-tu ?
… avec la main droite	Suis-moi
L’éventail placé près du cœur	Tu as gagné mon amour
Cacher ses yeux derrière l’éventail ouvert	Je t’aime
Rendre l’éventail fermé	M’aimes-tu ?
Le glisser sur la joue jusqu’au menton	Je vous aime
Porter l’éventail ouvert dans la main droite	Je suis très amoureuse
Placer l’éventail sur les lèvres	Embrasse-moi
Tourner l’éventail avec la main gauche	On nous voit
Le fermer complètement ouvert, lentement	Je promets de t’épouser
Le fermer en se touchant l’œil droit	Quand te verrai-je ?
Le nombre de branches ouvertes donne…	La réponse à la question
Mouvement menaçant, éventail fermé	Ne sois pas imprudent
Le placer ouvert devant l’oreille gauche	Cache notre secret
Approcher l’éventail autour des yeux	Je suis désolée
Ouvrir et fermer l’éventail plusieurs fois	Tu es cruel
Les mains jointes serrant l’éventail ouvert	Oublie-moi !
L’éventail derrière la tête, doigts tendus	Au revoir, adieu
Bouger l’éventail entre les mains	Je te hais

Quelques codes de l’éventail.

Il existait ainsi une trentaine de codes, assez pour faire passer ses sentiments et ses envies. La connaissance de ces codes est utile pour comprendre certains films, même si les mimiques

suggèrent parfois le message. Une sorte de cryptographie gestuelle…

Les argots et les jargons

Dans un genre différent, les argots et les jargons constituent une espèce de cryptographie orale. Il s'agit de communiquer au sein d'une communauté professionnelle, étudiante, religieuse, ethnique ou familiale, avec l'ambition de cacher en partie le sens de ses paroles aux personnes extérieures. Par exemple, « Il pleut ! » signifie dans certains argots « Attention danger ! » (ce sens semble naturel puisqu'il faut se couvrir en cas de pluie). Dans l'argot maçonnique, cette expression exprime en revanche un refus (le lien avec la pluie est plus éloigné cette fois). L'idée peut servir à un couple pour communiquer discrètement lors d'une soirée entre amis, comme Myr et Myroska, que nous avons rencontrés au chapitre précédent. Chacun est ainsi libre d'inventer ses codes et son argot à usage restreint.

Un des argots de la fin du XX^{e} siècle a été le verlan, qui consiste à prononcer les mots à l'envers, en inversant l'ordre des syllabes. Les monosyllabes, comme « fou », sont traitées en renversant la place de la ou des consonnes : « ouf ». Tous les mots ne sont pas forcément retournés comme dans « laisse béton », qui signifie « laisse tomber ». La clef de cet argot est si simple que tout le monde le comprend. Son usage est donc plus un marqueur identitaire qu'une véritable volonté de cacher.

Certains mots verlans, comme « beur » dérivé d'« arabe », sont quasiment tombés dans la langue courante. Sans doute ce glissement s'explique-t-il par l'inexistence d'un terme équivalent en français courant. En effet, « beur » a pris le sens de « jeune arabe né en France de parents maghrébins immigrés » et non d'arabe tout court.

Sur cet exemple, nous voyons que le français est perméable à l'argot et que ce dernier n'a pas qu'un rôle cryptique. Pour rester une langue cachée, le véritable argot doit être mobile. L'hermétisme se retrouve en mélangeant des mots d'origine

diverse, arabe ou anglaise le plus souvent de nos jours, et des argots à clefs comme le javanais.

Le javanais

Le javanais est un autre argot à clef – rien à voir avec la langue de Java ! Il s'agit d'un argot français inventé dans la seconde moitié du XIXe siècle. Selon certains historiens, il aurait été employé dans la rue par les prostituées et les voyous. Il se construit en insérant la syllabe supplémentaire « av » entre voyelles et consonnes, ainsi que devant le mot s'il commence par une voyelle.

Ainsi, « grosse » devient « gravosse » comme le savent tous les lecteurs de San-Antonio. Ici, le « e » muet est négligé comme il se doit. Cette règle souffre d'une exception avec le « y ». S'il est suivi d'une voyelle, il est traité comme une consonne : « moyen » devient « mavoyaven ». S'il est lui-même prononcé comme « i », il est traité comme une consonne suivie de la voyelle « i » : le mot « pays » est codé « pavayavis. Ainsi, « parler en javanais est une façon de chiffrer son message » devient « pavarlaver aven javavanavais avest avunave favaçavon dave chaviffraver savon mavessavagave ».

Ce Qu'il Faut Décrypter

La langue de feu

Voici un message écrit dans un javanais modifié, la langue de feu :

Dafiffaaficafilafe dafe cafomprafendrafe cafettafe lafangafue dafe fafeu

Avez-vous réussi à le décrypter ?

Les variantes sont innombrables. Une possibilité est de mélanger verlan et javanais ou, pire, la zorglangue inventée par André Franquin (1924-1997), le père de Spirou et de Gaston Lagaffe, pour son personnage de savant fou, l'ignoble Zorglub. Elle consiste à écrire les mots complètement à l'envers. Ainsi, « vive

Zorglub » devient « eviv Bulgroz ». La combinaison des deux est le sianavaj, langue difficile à maîtriser. Il existe encore d'autres combinaisons comme le largonji. Largonji signifie « jargon » en largonji. Ce mot décrit donc lui-même le procédé de chiffrement : la première lettre, si elle est une consonne, est remplacée par un « l », l'initiale se déplace en finale et sert de point de départ à un suffixe qui part du nom de la lettre (« ji » pour « j », « bé » pour « b »). Ainsi, « fou » se dit « louf » … ce qui a donné « loufoque », entré depuis dans la langue française.

Ce Qu'il Faut Décrypter

Le sianavaj

Voici un message écrit en sianavaj :

Ravelravap nave javavavanavais tasve tavacavilaved, avel averdnaverpmavoc averavocnave savulp

Saurez-vous le traduire en clair ?

Le navajo, le chacta… et le breton

Il est parfois inutile d'inventer de nouvelles langues pour communiquer secrètement : les langues existantes suffisent ! Chacun l'a vécu un jour ou l'autre : la meilleure façon de ne pas être compris au milieu d'une foule est de parler une langue étrangère. L'armée américaine fit sienne ce principe pendant la Seconde Guerre mondiale : elle eut l'idée d'engager 400 Navajos pour les transmissions sur le champ de bataille. Même les Indiens des autres ethnies étaient incapables de comprendre le navajo. De plus, les autorités avaient remarqué qu'aucun linguiste étranger n'était venu sur le sol américain l'étudier. Il était donc fort peu probable que quiconque soit capable de la comprendre, hormis les Navajos eux-mêmes et une poignée de linguistes américains. L'armée dut bien entendu enrichir la langue des Navajos de termes militaires comme « canon », « tank », « bombe », etc.

Deux Indiens navajos engagés par l'armée américaine transmettent des ordres par radio dans leur langue maternelle (juillet 1943). De par sa complexité, la langue navajo a servi de code secret aux Américains pendant la Seconde Guerre mondiale.

Puisqu'ils s'exprimaient dans leur propre langue, les Navajos constituaient des chiffreurs bien plus efficaces dans les situations de combat que n'importe quelle autre personne attachée au chiffrement, qui devait d'abord chiffrer ses messages avant de les envoyer en morse, messages qui devaient ensuite être traduits à l'autre bout de la ligne. Sans compter qu'avec l'angoisse du champ de bataille, les chiffreurs traditionnels commettaient des erreurs. Le temps gagné grâce aux codeurs navajos pouvait être vital pour des unités au combat. Ils furent déployés dans la guerre du Pacifique contre l'armée japonaise, qui ne semble jamais avoir compris leur langue. Leur action étant couverte par le secret Défense, comme toujours en la matière, elle ne fut reconnue que tardivement.

En l'occurence, l'emploi de locuteurs spécialisés en temps de guerre n'a rien d'original. L'armée française utilisa des Bretons pendant la guerre d'Indochine. De même, les Américains employèrent les Chactas, une tribu amérindienne vivant dans le sud-est des États-Unis, pendant la Première Guerre mondiale puis la Seconde, mais l'histoire a davantage retenu les Navajos dans ce rôle.

La langue des oiseaux

À bien y réfléchir, nul besoin de faire appel à des langues étrangères ou à des dialectes pour chiffrer des messages. En

jouant sur les homophonies, c'est-à-dire sur les sonorités des mots, il est possible de déguiser des messages à l'intérieur même de la langue courante. Cette pratique ancienne – les alchimistes y avaient recours – porte le nom de langue des oiseaux. Pourquoi cette référence à des animaux ? Parce que, dans l'Antiquité, les oiseaux étaient vus comme les messagers des dieux. On observait leur vol et écoutait leur chant pour prédire l'avenir.

Des exemples de langue des oiseaux ? Prenez la phrase « Ce message ne peut être compris que par des saints ». Sa fin peut être entendue de plusieurs manières : des saints, dessins ou desseins ? De même, l'expression « au-delà des mots » peut être entendue « au-delà des maux » et « la mère l'oie » comme « l'amère loi ».

Le français fourmille d'homophonies possibles : mal, mâle, maux, mots, seins, saints, seings, sot, seau, sceau, chat, chas, shah, etc. C'est ainsi que le Moyen Âge inventa le chat pour désigner le sexe féminin, par identification avec le chas, qui désigne le trou d'une aiguille. Le chat fut ensuite féminisé et même familiarisé, comme l'illustrent les déclarations d'un certain président américain…

Nous pouvons multiplier à l'infini les exemples de ce qui peut être un jeu, avec ou sans volonté de cacher, comme ce nom d'hôtel *Au Lion d'Or* (au lit, on dort), ce texte « un mets sage se crée » ou l'art goth, tout sauf argotique. Cette façon de jouer avec les mots fait penser à Jacques Lacan (1901-1981) pour qui l'inconscient s'exprimerait à travers ce type de double sens. Le meilleur exemple étant cet échange entre lui et un patient : « Je persévère… Vous avez dit père sévère ? ». Entre les oiseaux messagers des dieux et l'inconscient, il n'y a qu'un pas et l'annonce d'une tumeur (tu meurs) ne peut se faire à la légère !

Les SMS

Lisez-vous ce livre avec votre téléphone portable à proximité ? Si oui, combien de fois avez-vous interrompu votre lecture pour répondre à un texto ? Il y a toutes les chances pour que, ce faisant, vous ayez parlé l'« oiseau » sans le savoir. Le langage SMS (*short message service*) s'inspire en effet en partie de la langue

des oiseaux. Pas pour les « bjr » (bonjour), « slt » (salut) ou « mdr » (mort de rire) qui sont de simples abréviations, mais pour des mots à prononcer pour les comprendre comme « g » (j'ai), « c » (c'est), « l » (elle), « ajt » (agité), « a12c4 » (à un de ces quatre), « koi29 » (quoi de neuf ?), « lv » (élevé), « c1k » (c'est un cas), « nrv » (énervé), « ht » (acheté), « toqp » (t'es occupé ?), « fac » (effacé), « 1 kfé » (un café), etc. Bien sûr, les règles sont diverses, si bien que nous obtenons : « kic » (qui c'est ?), « keske » (qu'est-ce que) et tous les mélanges que l'on veut), etc. Cela permet des échanges sibyllins comme : koi29, rvmln, ki, ln, ekoi, lacd, aki, arv, ema, lcnrv, e, c1k, etc. (quoi de neuf ? Hervé aime Hélène, qui ?, Hélène, et quoi ?, elle a cédé ?, à qui , à Hervé !, et Emma ?, Elle s'est énervée, et ?, c'est un cas).

Le comble de l'élégance concerne les SMS de rupture, au point que des concours ont été organisés sur le sujet, mais peut-être vaut-il mieux être clair et bref pour que la fin soit moins douloureuse : « jtm+by » (je t'aime plus, bye bye).

4

Les chiffres par substitution

Les précédents chapitres étaient une mise en bouche, un aperçu historique et pluriel des méthodes de chiffrement. Maintenant, finie la récréation ! Pour devenir de véritables décrypteurs amateurs, il est temps d'entrer un peu plus dans le secret… des codes secrets. Ceux qui vont nous intéresser plus particulièrement ici sont les chiffres par substitution.

Vous vous souvenez de César chiffrant ses messages afin qu'ils ne tombent pas entre les mains des barbares germaniques ? Les différents chiffres que nous verrons sont des extensions plus ou moins sophistiquées de son code, qui consiste à remplacer chaque lettre par un symbole. Mais rassurez-vous, le plaisir du jeu intellectuel ne restera jamais très loin de notre cheminement. Même lorsqu'un tueur en série nous mettra au défi…

Ave césar

L'idée de substituer des symboles aux lettres vient de l'Antiquité, puisque Jules César chiffrait déjà avec cette méthode, comme nous l'avons déjà vu. En le généralisant à peine, le chiffre de César consiste à décaler les lettres du message d'une façon convenue à l'avance. La méthode des fréquences d'Al-Kindi permet de le décrypter très rapidement,

si l'on part du principe que la lettre la plus fréquente est la voyelle E (en français et en anglais). Précisons cette idée sur le message suivant :

PRZRFFNTRRFGGERFSNPVYRNQRPBQRE

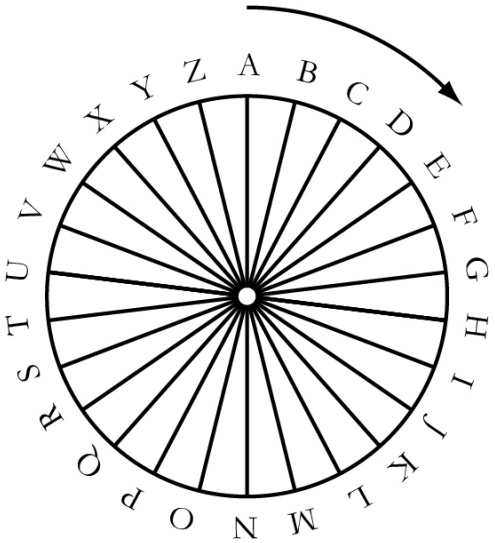
La lettre la plus fréquente y est le R, qui doit représenter le E si ce message a été chiffré par un césar (le chiffre, pas la personne). Le décalage est donc de 13. En l'appliquant à l'envers, on trouve :

CEMESSAGEESTTRESFACILEADECODER

Le fait que cette phrase ait un sens montre que notre hypothèse est correcte. Ce chiffre est nommé Rot13 (rotation de 13), car il s'agit d'une rotation, plus que d'un décalage de treize lettres. Pourquoi une rotation ? Pour le comprendre, représentez-vous les lettres sur un cercle. Les 26 lettres correspondent à l'angle total de 360° (voir la figure p. suivante). Rot13 équivaut à la symétrie par rapport au centre. Compris ?

Puisque Rot13 revient à prendre le symétrique d'une lettre sur le cercle, pour déchiffrer un message, il suffira de l'appliquer une nouvelle fois. Deux symétries centrales ramènent au point de départ. L'avantage du Rot13 par rapport à n'importe quelle autre rotation est évident : le codage et le décodage se réalisent de la même manière.

Cette particularité fait que ce chiffre, pourtant facile à décrypter, est utilisé pour cacher certains messages sur Internet. Bien entendu, il ne peut servir sérieusement à garder un secret, mais il reste intéressant pour ne pas dévoiler trop vite les solutions de jeux, les fins de films ou ne pas dévoiler l'intrigue d'une série. L'usage est donc identique aux indications données en fin d'ouvrage, en solution des CQFD.



Le décalage dans le chiffre de César correspond à une rotation. Si les lettres sont tracées sur un cercle divisé en 26 parts égales, un décalage de 1 correspond à une rotation d'une part, un décalage de 2 à une rotation de deux parts, etc. Une rotation de 13 correspond à la symétrie par rapport au centre. Si on l'applique deux fois, on revient à la lettre initiale. Chiffrement et déchiffrement s'opèrent donc de même.

Ce Qu'il Faut Décrypter

Les chiffres d'Hervé et d'Hélène

Hélène et Hervé ont chacun leur chiffre, voici un de leurs échanges :

LIPIRIVIRHIDZSYWHMQERGLISRDILIYVIWFMWIWVZ
FCEEQTFDKUGUNP

Que se disent-ils ?

Ce Qu'il Faut Décrypter

Le chiffre de Cassis

Le cryptogramme suivant a été chiffré au moyen du chiffre de Cassis :

130009250021 17101614 22 24040912 030016130014 2216

0710242207

Saurez-vous le lire ?

Le grand bazar

Et si l'alphabet de substitution n'était pas l'alphabet classique bien ordonné ? Et si on remplaçait les lettres de l'alphabet en les jetant dans une poche de scrabble et en les piochant ensuite au hasard une par une ? Un tel chiffre est toujours une « substitution alphabétique ». Imaginons que notre alphabet de remplacement soit « MOTIZNGYLWFHJCSXRBDKVPQAUE » (vous noterez que chaque lettre figure exactement une fois, ni plus ni moins). La règle de substitution associée est la suivante : à A on fait correspondre M, à B, O, etc. Elle peut s'inscrire dans un tableau.

A	B	C	D	E	F	G	H	I	J	K	L	M
M	O	T	I	Z	N	G	Y	L	W	F	H	J

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
C	S	X	R	B	D	K	V	P	Q	A	U	E

Une substitution alphabétique consiste à écrire l'alphabet dans un ordre différent. Ici, aux lettres de la première ligne correspondent celles de la seconde.

La règle d'application de ce chiffre est que chaque lettre de la première ligne doit être remplacée par la lettre correspondante dans la seconde ligne. Le chiffrement de la phrase « voici comment coder » peut se faire dans un tableau.

V	O	I	C	I	C	O	M	M	E
P	S	L	T	L	T	S	J	J	Z

N	T	C	O	D	E	R
C	K	T	S	I	Z	B

Exemple de chiffrement : le texte clair figure en première ligne, le texte chiffré en seconde.

Pour déchiffrer le message, il suffit de lire le tableau à l'envers, ce qui est plus simple en construisant un nouveau tableau :

A	B	C	D	E	F	G	H	I	J	K	L	M
X	R	N	S	Z	K	G	L	D	M	T	I	A

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
F	B	V	W	Q	O	C	Y	U	J	P	H	E

Tableau de déchiffrement du chiffre précédent.

Pour le créer, nous avons cherché le A dans la seconde ligne du premier tableau et reporté la lettre trouvée en seconde ligne de ce nouveau tableau, et ainsi de suite. Le déchiffrement se fait alors de même que le chiffrement.

V	C	C	S	V	P	Z	H	Z	D
U	N	N	O	U	V	E	L	E	S

D	M	L	I	Z	T	S	I	Z
S	A	I	D	E	C	O	D	E

Exemple de déchiffrement.

Sur une des chemises pour le chevalier de Rohan, il était écrit :
MG DULHXCCLGU GHJ YXUJ LM CT ULGE ALJ
Quelle est la version en clair du texte ?

Un moyen mnémotechnique

Un obstacle demeure : il n'est pas simple de retenir une suite de 26 lettres désordonnées comme « MOTIZNGYLWFHJCSXRBDKVPQAUE ». Pour l'apprendre, mieux vaut mémoriser quelque chose qui la résume, comme un petit texte ou une poésie, par exemple « L'Albatros » de Baudelaire :

> Souvent, pour s'amuser, les hommes d'équipage Prennent des albatros, vastes oiseaux des mers,
> Qui suivent, indolents compagnons de voyage,
> Le navire glissant sur les gouffres amers.

Écrivons les lettres du poème en supprimant les doublons, ajoutons ensuite les lettres manquantes. Nous obtenons la liste de lettres « SOUVENTPRAMLHDQIGBXCYFJKWZ » et la correspondance (différente de l'exemple précédent) :

A	B	C	D	E	F	G	H	I	J	K	L	M
S	O	U	V	E	N	T	P	R	A	M	L	H

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
D	Q	I	G	B	X	C	Y	F	J	K	W	Z

Tableau de chiffrement lié à l'Albatros.

Ce Qu'il Faut Décrypter

Un message chiffré par l'Albatros

Le message suivant a été chiffré au moyen du chiffre de l'Albatros :

FQRUR YDUPR NNBEC BEXNS ROLE
Serez-vous aussi poète que son auteur ?

Comment faire si l'on souhaite que notre chiffre alphabétique soit réversible comme Rot13, c'est-à-dire que si A se chiffre en P, alors P se chiffre en A ? Le bénéfice des chiffres réversibles est d'économiser de l'espace mémoire mental. Ils peuvent se construire facilement en choisissant un premier couple de lettres au hasard, comme (A, F), puis un autre parmi les lettres restantes, comme (S, H), et ainsi de suite. Cela donne par exemple :

A	S	B	U	D	L	E	I	T	O	C	R	Q
F	H	G	J	M	X	V	N	P	W	Z	K	Y

Ainsi, « soyez-prêts demain à huit heures » se chiffre en :

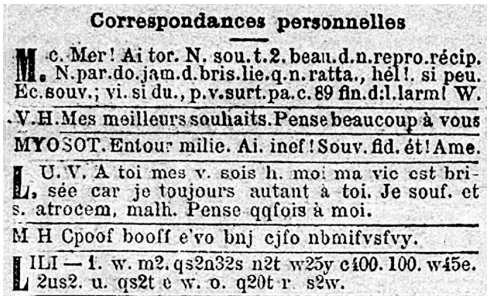
HWQVC TKVPH MVDFN IFSJN PSVJK VH

L'inconvénient de toutes ces méthodes est qu'une lettre n'est jamais chiffrée par elle-même, ce qui affaiblit le code vis-à-vis d'une attaque par la méthode du mot probable, comme nous le verrons plus loin dans le cas de la machine Enigma, dont c'était l'une des faiblesses. Pour corriger ce défaut, nous pouvons d'abord choisir un nombre pair de lettres se chiffrant par elles-mêmes, puis continuer en choisissant les couples de lettres au hasard.

Les correspondances personnelles du *Figaro*

Les principes des codes de substitution étant exposés, il est temps de nous faire la main sur des exemples. Et si nous les tirions des pages « Correspondances personnelles » du *Figaro*, de la fin du XIX^e^ siècle ? Rappelez-vous, ces pages servaient à des couples illégitimes pour communiquer et furent à l'origine

de la vocation du célèbre cryptologue Étienne Bazeries. Voici la rubrique du premier janvier 1890. J'ai choisi cette date car elle laissait espérer la présence de mots probables comme « vœux » ou « bonne année ».



Correspondances personnelles

M c. Mer ! Ai tor. N. sou. t. 2. beau. d. n. repro. récip. N. par. do. jam. d. bris. lie. q. n. ratta., hél !. si peu. Ec. souv.; vi. si du., p. v. surt. pa. c. 89 fin. d: l. larm ! W.

. V. H. Mes meilleurs souhaits. Pense beaucoup à vous

MYOSOT. Entour milie. Ai. inef ! Souv. fid. ét ! Ame.

L U. V. A toi mes v. sois h. moi ma vie est brisée car je toujours autant à toi. Je souf. et s. atrocem, malh. Pense qqfois à moi.

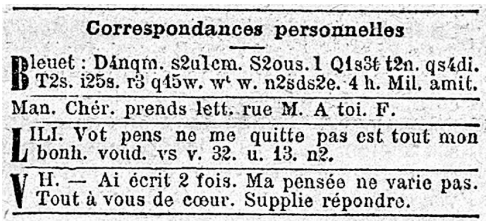
M H Cpoof booff e'vo bnj cjfo nbmifvsfvy.

L ILI — 1. w. m2. qs2n32s n2t w25y c400. 100. w45e. 2us2. u. qs2t e w. o. q20t r. s2w.

Extrait de la rubrique « Correspondances personnelles » du 1er janvier 1890 dans le *Figaro*.

Parmi un grand nombre de messages écrits en style télégraphique, nous en trouvons deux manifestement chiffrés. Dans le premier, « bonne année » est devenu cpoof booff. Autrement dit, il s'agit d'un simple chiffre de César et le tout signifie : « Bonne année d'un ami bien malheureux ».

Le message suivant (d'indicatif LILI) est bien plus intéressant à décrypter. De prime abord, nous pouvons juste penser que le chiffre 2 représente E, du moins si la méthode de chiffrement mobilisée est une substitution alphabétique car il s'agit du symbole majoritaire. Heureusement, en feuilletant le *Figaro* des jours suivants, nous rencontrons un grand nombre de messages sous le même indicatif LILI. Le 12 janvier est publié un message à moitié chiffré, une erreur classique de chiffrement.



Correspondances personnelles

Bleuet : D4nqm. s2ulcm. S2ous. 1 Q1s3t t2n. qs4di. T2s. i25s. r3 q45w. w[t] w. n2sds2e. 4 h. Mil. amit.

Man. Chér. prends lett. rue M. A toi. F.

LILI. Vot pens ne me quitte pas est tout mon bonh. voud. vs v. 32. u. 13. n2.

VH. — Ai écrit 2 fois. Ma pensée ne varie pas. Tout à vous de cœur. Supplie répondre.

La même rubrique, le 12 janvier 1890.

Écrit en style télégraphique, le message commence par « votre pensée ne me quitte pas, est tout mon bonheur, voudrais vous voir », la suite qu'on veut cacher est « 32. u. 13. n2 ». La disposition des deux 2 nous fait penser à « je t'aime » si i et j sont assimilés comme ils le sont en latin. Les chiffres 1, 2 et 3 représentent les voyelles A, E et I, les lettres U et N représentent T et M. La méthode de chiffrement semble être de représenter chaque voyelle par son numéro d'ordre et chaque consonne par la lettre qui la suit. Pour vérifier cette hypothèse, revenons au message du premier janvier :

1.w. m2. qs2n32s n2t w25y c400. 100. w45e. 2us2. u. qs2t e w. o. q20t r s2w.

En le déchiffrant selon la méthode que nous venons d'exposer, on obtient une phrase en style télégraphique :

a v le premier mes veux bonn ann voud etre t pres d v n pens q rev

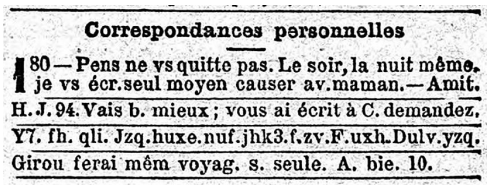
ce qui signifie probablement :

À vous le premier, mes vœux de bonne année. Je voudrais être tout près de vous. Ne pense qu'un rêve !

Même si une erreur a pu se glisser dans la dernière phrase, le sens des deux premières prouve que notre hypothèse est correcte. De façon étonnante, la méthode de décryptement fonctionne pour un autre message du 12 janvier, celui portant l'indicatif Bleuet :

Complètement rétabli. Rentre à Paris semaine prochaine, je serai heureux de pouvoir vous voir mercredi 4 h. Mille amitiés.

La plupart des textes chiffrés sont de ces deux formes : décalage de César ou code Lili. Il faut chercher jusqu'au 23 janvier pour trouver autre chose, sous l'indicatif Y7.



Correspondances personnelles

180 — Pens ne vs quitte pas. Le soir, la nuit même, je vs écr. seul moyen causer av. maman. — Amit.
H. J. 94. Vais b. mieux ; vous ai écrit à C. demandez.
Y7. fh. qli. Jzq.huxe.nuf.jhk3.f.zv.F.uxh.Dulv.yzq.
Girou ferai mêm voyag. s. seule. A. bie. 10.

Rubrique du 23 janvier 1890.

On lit des messages étiquetés pareillement les 30 et 31 janvier :

Y7. gqn. utth. Fhu3y. lked. 3zn. Fzxr. uxh. Hud. dqf.
Y7. julg. qlxqv. ufhzlsud.z.lg.Nuf.l.jhked.j.ugjqkl. Jnefk. rkm. ve. 3klv. Gkq. Xzn3, jz. Qli. – F.z.

L'absence des premières lettres de l'alphabet (a, b et c), la prédominance de la lettre u et l'étude des fréquences des lettres suggèrent le chiffre « atbash » qui renverse l'alphabet, z représentant *a*, y, *b*, etc. Toutefois, il est nécessaire d'assimiler v et w dans notre cas, ce qui est classique.

Ce chiffre est très ancien puisqu'on le trouve déjà dans la Bible hébraïque – son nom vient d'ailleurs de l'hébreu. Il désigne les initiales des deux premières et des deux dernières lettres de l'alphabet mises dans l'ordre où elles se correspondent dans le chiffre, soit : aleph, tav, beth, shin. De plus, ici, le 3 a été ajouté pour chiffrer « m » qui, sinon, se chiffrerait en lui-même, ce qui ne serait pourtant pas une faiblesse particulière, au contraire.

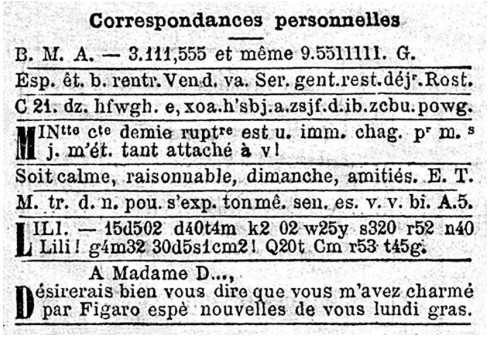
Le décryptement ne se limite pas à cette simple substitution car il faut ensuite traduire le style télégraphique ! Ainsi, le message du 31, même s'il se décrypte d'abord de cette façon, reste ensuite énigmatique, avec des termes comme espion et homme du monde :

Pens incid etrange v a ns let n prouv p espion pluto hom du mond sov calm pa inq - T.a.

Ce Qu'il Faut Décrypter

Les correspondances du 20 février 1890

Voici les correspondances personnelles du *Figaro* du 20 février 1890 :



Correspondances personnelles

B. M. A. — 3.111,555 et même 9.5511111. G.

Esp. êt. b. rentr. Vend. va. Ser. gent. rest. déjr. Rost.

C 21. dz. hfwgh. e, xoa. h'sbj. a. zsjf. d. ib. zcbu. powg.

MINtte cte demie ruptre est u. imm. chag. pr m. s j. m'ét. tant attaché à v!

Soit calme, raisonnable, dimanche, amitiés. E. T.

M. tr. d. n. pou. s'exp. tonmê. sen. es. v. v. bi. A.5.

LILI. — 15d502 d40t4m k2 02 w25y s320 r52 n40 Lili! g4m32 30d5s1cm2! Q20t Cm r53 t45g.

A Madame D...,

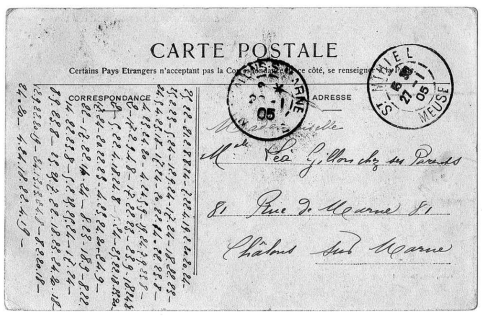
Désirerais bien vous dire que vous m'avez charmé par Figaro espè nouvelles de vous lundi gras.

Saurez-vous décrypter les messages d'indicatifs C 21 et LILI ?

Les cartes à Léa

Pour achever de vous convaincre que la substitution alphabétique simple n'incarne pas la méthode idéale pour protéger un secret, voici une carte postale. Envoyée à une jeune fille résidant chez ses parents, elle est datée du 1er janvier 1905. Cette carte a été dénichée dans une brocante par un passionné, membre comme moi de l'ARCSI (Association des réservistes du chiffre et de la sécurité de l'information), Daniel Tant. Elle est chiffrée sans doute pour éviter la lecture des parents de la jeune fille, même si le procédé ne pouvait qu'éveiller leurs soupçons… Je vais vous montrer d'ailleurs comment ils auraient pu la lire sans mal !

Saint-Mihiel. — Église Saint-Michel et la Division.



CARTE POSTALE

CORRESPONDANCE

ADRESSE

Mlle Léa Gillon chez ses Parents

81 Rue de Marne 81

Châlons sur Marne

MEUSE

Le texte est constitué de nombres entre 2 et 25, qui représentent sans doute des lettres de l'alphabet, séparés par des points et des tirets. Les tirets isolent probablement les mots. Voici la reproduction du texte, les tirets ayant été remplacés par des espaces :

> 25.22 21.2.8.8.24 7.22.4.19.2.20.20.24 25.2.23 5.24 12.9.24 17.24 18.22.23 24.5.4.23.18 17.24 20.22.14.22.23.8 4.23.24.20 4.24.5.9 19.24.7.9.23.8 2 17.2.9.4.8 17.22.23 23.9 18.24.8 2 5.22.4.18.24.8 5.24 25.22.18.23.20 17.24 20.22.23 4.23.24.20 24.9 22 17.22.14.24 8.23 18.9 8.22.14.22.23.8 5.2.25.25.24 17.24 8.9.23.8 23.25.7.22.18.23.24.20.18 12.9.22.20.19 24.13.13.24.8 8.2.20.18 24.20 4.24.18.22.4.19 22.9 4.24.14.2.23.4 25.2.20 22.20.21.24 22.19.2.4.24 18.2.9.18 22 18.2.23

On remarque rapidement que le numéro 24 est majoritaire parmi les nombres. Il représente sans doute le E. Un mot à l'avant-dernière ligne se trouve alors à moitié décrypté. Il s'agit de « 24.13.13.24.8 ». Le numéro 13 répété entre deux E ne peut être qu'une consonne, plus précisément L. On en déduit que ce mot est « elles ». Le suivant est alors probablement « sont ».

Le chiffre s'écroule progressivement. En particulier, la formule de politesse est « tout à toi ». Finalement, on obtient le texte :

> Ma gosse, pardonne-moi ce que je t'ai écrit, je n'avais rien reçu depuis 2 jours. J'ai eu tes 2 cartes ce matin. Je n'ai rien eu à ja*e. Si tu savais comme je suis impatient quand elles sont en retard. Au revoir mon ange. Tout à toi.

L'étoile dans le texte représente une lettre que je n'ai pas réussi à décrypter, sans doute une erreur de chiffrement.

Ce Qu'il Faut Décrypter

L'épilogue des cartes à Léa

La collection des cartes à Léa en comprend trois autres.
1er février 1905 :

25.22 13.24.22 22.19.2.4.24.24 17.24 18.22.23.25.24 19.24 18.2.9.18.24 25.2.20 22.25.24 24.18 8.2.9.10.10.4.24 13.2.23.20 19.24 18.2.23 18.22 7.3.2.18.2.21.4.22.7.3.23.24 24.8.18 22.13.22 18.24.18.24 19.24 25.2.20 13.23.18 25.2.20 7.4.24.25.23.24.4 4.24.21.22.4.19 13.24 25.22.18.23.20 24.8.18 7.2.9.4 18.2.23 12.9.24 17.24 5.3.24.4.23 18.22.20.18 22.19.23.24.9 25.2.20 22.20.21.24 15.23.24.20 22.23.25.24 9.20 25.23.13.13.23.2.20 19.24 15.22.23.8.24.4.8

9 février 1905 :

25.2.20 22.25.2.9.4 17.24 8.9.23.8 22.9.8.8.23 23.25.7.22.18.23.24.20.18 19.24 18.24 4.24.14.2.23.4 25.22.23.8 7.2.9.4.12.9.2.23 18.24.20.20.9.23.24.8 20.2.9.8 4.22.18.18.4.22.7.24.4.2.20.8 13.24 18.24.25.7.8 7.24.4.19.9 12.9.22.20.19 17.24 8.24.4.22.23.8 13.23.15.4.24 5.2.25.25.24.20.18 5.24 10.22.23.18 23.13 12.9.24 17.24 4.24.5.2.23.8 18.24.8 5.22.4.18.24.8 12.9.24 13.24 8.2.23.4 18.22.20.19.23.8 12.9.24 17.24 13.24.8 4.24.5.24.14.22.23.8 13.24 25.22.18.23.20 9.20 15.2.20 15.22.23.8.24.4

18 février 1905 :

25.22 5.3.24.4.24 13.24.22 17.24 8.9.23.8 18.4.24.8 7.24.23.20.24 24.20 13.23.8.22.20.18 18.22 5.22.4.18.24 17.24 20.24 7.24.20.8.22.23.8 7.22.8 22.14.2.23.4 25.24.4.23.18.24 13.24.8 4.24.7.4.2.5.3.24.8 12.9.24 18.9 25.22.19.4.24.8.8.24.8 8.23 17.24 20.24 18.22.23 7.22.8 8.23 15.23.24.20 24.25.15.4.22.8.8.24 22 14.24.4.18.9.8 5.24.8.18 12.9.24 20.2.9.8 20.22.14.2.20.8 7.22.8 24.18.24 8.24.9.13.8 8.23 13.2.20.21.18.24.25.7.8 5.24 20.24.8.18 7.22.8 10.22.9.18.24 19.24 18.22.14.2.23.4 22.18.18.24.20.19.9 19.23.25.22.20.5.3.24 14.2.23.13.22 13.22 4.24.5.2.25.7.24.20.8.24 22.19.23.24.9

Saurez-vous les décrypter ?

Les digrammes disent tout

Comment décrypter des chiffres plus complexes ? Dans les exemples précédents, le décryptement était simplifié car le découpage des mots était respecté. Transmettre ainsi de façon structurée son message constitue une erreur majeure, commise par les apprentis chiffreurs. Et si le message était envoyé en vrac ? Cela rendrait la tâche du décrypteur un peu plus ardue, mais pas impossible : de façon générale, toute substitution alphabétique est déchiffrable grâce à la méthode des fréquences, à condition qu'on dispose d'un texte chiffré suffisamment long.

En voici la preuve avec le message :

BTUFM ZBZFS YWUFK FSFSC BTVYU FZFZF SYFWU KFJUB VYMBJ RVUWY VZVMF UZBAF YCRKF KFMDU FGWFN SFMTR WUKFS RKFUK FMAFM MBPFM SRKFM BJFSW NFMWH MYVYW YVRNB ZTCBH FYVGW F

Ce message était au départ rédigé d'une traite (les lettres étaient collées les unes aux autres), mais je l'ai découpé par groupes de cinq lettres, comme c'était le cas sur les télégrammes (la raison était que les télégrammes étaient facturés au nombre de « mots » de cinq lettres). Remarquez que ce découpage rend le texte plus facilement transmissible par un opérateur. Pour décrypter le message, calculons le nombre d'occurrences de chaque lettre, puis leurs fréquences en divisant par le nombre total de lettres, qui est de 136. La comparaison de ces deux tableaux montre que F correspond à E. Les autres lettres fréquentes sont B, K, M, S, U, V, W et Y. Parmi celles-ci se trouvent sûrement A, I, N, R, S et U. Rien n'étant évident pour l'instant, remplaçons simplement F par E.

L'analyse des fréquences des lettres ne suffit pas pour décrypter un texte aussi court. Il est nécessaire de tenir compte des groupes de deux lettres (les digrammes) les plus fréquents. Comme nous avons déjà repéré le E, étudions les digrammes contenant cette lettre.

ES	DE	LE	EN	RE	ER	TE	EL	SE	ET
ME	EM	IE	ED	NE	EC	EE	UE	CE	EU

Digrammes contenant E les plus fréquents en français, dans l'ordre. Les premiers sont trois fois plus fréquents que les derniers.

Dans le texte chiffré, nous rencontrons huit fois KF et FM, six fois FS et quatre fois UF, les autres occurrences étant trop réduites pour être interprétées. Cela laisse supposer que K est D, ce que la fréquence de K ne contredit pas, puisqu'elle est de 5,88 % dans le texte codé, contre 4,18 % de D dans un texte ordinaire. Le même type de raisonnement conduit à penser que M est S. En faisant l'hypothèse probable que B est A, nous obtenons en gras la partie de message décrypté :

ATU**ES** Z**A**Z**E**S YWU**ED** **E**S**E**SC **A**TVYU **E**Z**E**Z**E** SY**E**WU **DE**JU**A** VY**SA**J RVUWY VZV**SE** UZ**A**A**E** YCR**DE** **DES**DU **E**GW**E**N S**ES**TR WU**DE**S R**DE**U**D** **ES**A**ES** **SA**P**ES** SR**DES** **A**J**E**SW N**ES**WH **S**YVYW YVRN**A** ZTC**A**H **E**YVGW **E**

Il est logique de penser que S représente N, cela correspond aussi bien aux fréquences de digrammes qu'à celles des lettres. Cependant, cette hypothèse aboutit à une impasse à cause des troisième et quatrième groupes de lettres du texte, qui donneraient « EDENEN », une suite peu crédible. Après cet essai, nous sommes amenés à essayer C. De même, la suite « **E**Z**E**Z**E** » fait penser que Z représente L, ce qui est crédible au niveau des fréquences. Nous obtenons :

ATU**ES LALEC** YWU**ED ECEC**C **A**TVYU **ELELE C**Y**E**WU **DE**JU**A** VY**SA**J RVUWY V**L**V**SE** U**LA**A**E** YCR**DE DES**DU **E**GW**E**N **CES**TR WU**DE**S R**DE**U**D ES**A**ES SA**PES **C**R**DES A**J**E**SW N**ES**WH **S**YVYW YVRN**A L**TC**A**H **E**YVGW **E**

Les consonnes à leur place

Aucun mot n'apparaît de façon évidente dans ce début de décryptement. Cependant, le premier mot laisse penser que T représente une consonne. Sa fréquence est de 3 %, ce qui nous amène à essayer P. Il serait alors logique que U soit R, ce qui formerait le mot « APRES ». Des mots cohérents apparaissent alors au début du message :

APRES LA LEC YW**RE DE CE C**C **AP**VY**R ELELE C**Y**E**W**R DE**J**RA** VY**SA**J RV**R**WY V**L**V**SE RLA**A**E** YCR**DE DES**D**R E**GW**E**N **CESP**R W**RDE**S R**DERD ES**A**ES SA**P**ES **C**R**DES A**J**E**SW N**ES**WH **S**YVYW YVRN**A LP**C**A**H **E**YVGW **E**

Nous pouvons commencer à jouer aux devinettes, en tenant compte des fréquences bien entendu. Il apparaît que Y est probablement T et W, U ce qui forme le mot « LECTURE » d'où :

APRES LA LECTURE DE CE CCA**P**V**TRE LE LECTEUR DE**J**RA**V**T SA**J RV**RUT** V**L**V**SE RLA**A**E TCR**DE DES**D**R E**G**UE**N **CESP**R **URDE**S R**DERD ES**A**ES SA**P**ES **C**R **DES A**J**E**S**U** N**ESU**H **ST**V**TU T**VRN**A LP**C**A**H **ET**VG**U E**

À ce stade, des pans entiers du code s'effondrent. Ainsi le mot « **C**C**AP**V**TRE** » est « CHAPITRE », les mots « DEVRAIT », « SAVOIR », « METHODE », « FREQUENCES », « DECODER », « MESSAGES » et « SUBSTITUTION » apparaissent ensuite successivement, d'où le message décrypté :

Après la lecture de ce chapitre, le lecteur devrait savoir utiliser la méthode des fréquences pour décoder des messages codés avec une substitution alphabétique.

L’exemple que nous venons de détailler est typique de la façon dont un chiffre par substitution mono-alphabétique s’écroule progressivement, comme un mur que l’on mine. Tout texte chiffré de la même manière sera ensuite décrypté rapidement.

Ce Qu’il Faut Décrypter

Un message littéraire

Nous avons intercepté le message suivant entre deux critiques littéraires :

OGNJL VDKXJ LHWFL WWLPH WIDHO WKADW WPFHJ PWKAD WQJDH PGLPX OBGTX VVWHW LNWOW IDHOW KADWG QQGHP XWLPG OEXKP JXHWO XPPWH GXHWW PNJLK PXPDW DLFWL HWADW OJLQW DPNWH LWHOW FHJPW KADWL WKPQG KDLFW LHWXO NGHGN PWHXK WQODP JPDLP BQWTW QWHKJ LLGFW KTWHJ SGL

En trouverez-vous le sens, sachant que nos critiques s’intéressent au burlesque ?

Chiffrer avec des digrammes

J’ai pioché l’exemple suivant dans un registre un peu plus complexe. Ce n’est pas un exemple pour vous entraîner, juste pour vous montrer un type de chiffrement atypique : son originalité est de recourir à des digrammes (groupes de deux lettres). Il est extrait d’une correspondance, datée de 1642, entre le secrétaire de Strasbourg et les agents de la ville à Paris. Cet extrait, qui fait partie des archives de la ville de Strasbourg, illustre l’évolution des titres : ces personnages (secrétaire et agents) avaient des fonctions importantes à l’époque ! De plus, Strasbourg n’était pas encore une ville française (elle l’est devenue en 1648), mais avait des agents à Paris afin de se renseigner sur l’évolution de la situation. Le texte relate donc l’arrivée d’un diplomate à la cour de France.

Même si le contexte historique est intéressant, je m’en tiendrai à l’évolution de la cryptographie. De ce point de vue,

la missive, découverte dans les archives de Strasbourg, prouve qu'à l'époque, certains concepteurs de chiffres s'étaient rendu compte que l'emploi de symboles ésotériques ne servait à rien, ce qui préfigurait le passage au chiffrement à l'aide de nombres. Des parties chiffrées de la lettre sont déchiffrées, ce qui m'a permis de reconstituer la table de chiffrement.

Lettre partiellement chiffrée, et déchiffrée (au-dessus).

Ce chiffre est accompagné d'un nomenclateur (c'est-à-dire d'un code pour désigner d'autres éléments que des lettres, des noms propres entiers, par exemple) fonctionnant également avec des couples de chiffres. Figurent ainsi 25 et 39, désignant des personnages de la Cour semble-t-il, dont un certain Noyers (pour 25). L'idée était bonne mais gâchée par un mélange de clair et de chiffré, ainsi que par le découpage entre les lettres. Il aurait été préférable de grouper les lettres autrement. De plus, le début de la phrase « à mon arrivée à la Cour, j'y ai fort entretenu xxxxxxx qui m'a témoigné du regret » invite à chercher qui est ce personnage dont le nom fait sept lettres.

clair	*a*	*b*	*c*	*d*	*e*	*f*	*g*	*i*	*l*
chiffré	*bo*	*ao*	*rp*	*gq*	*fs*	*es*	*lg*	*tx*	*mz*
clair	*m*	*n*	*o*	*p*	*r*	*s*	*t*	*u*	
chiffré	*lz*	*hw*	*ab*	*rc*	*cp*	*ef*	*ix*	*ky*	

Reconstitution de la table de chiffrement d'une lettre déchiffrée ; chaque lettre doit se chiffrer par le digramme situé en dessous.

Ce Qu'il Faut Décrypter

Un message de Paris à Strasbourg

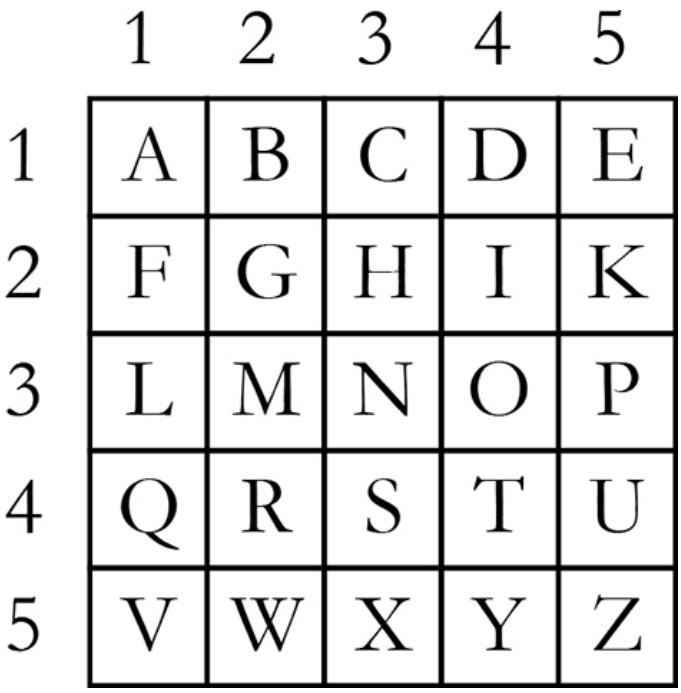
Nous avons intercepté le message suivant qui utilise le chiffre digrammique (fondé sur des digrammes) de Strasbourg :

Bien arrivé à la Cour où tout n'est que fêtes et bonheurs,
Lz fsest xfscpky abk yefgq fsmzb olgbo cpgqfs.
Votre dévoué.

Saurez-vous le décrypter ?

Carré-ment bien

Tout aspirant cryptologue se doit de connaître ses classiques. Saviez-vous que le chiffre de César n'est pas le seul chiffre de substitution de l'Antiquité à nous être parvenu ? Il y a aussi le carré de Polybe, qui tire également son nom d'un général, mais grec cette fois. Après avoir contribué à la destruction finale de Carthage, Polybe (200-155 ans avant notre ère environ) écrivit un traité de stratégie, dans lequel on trouve le système de transmission connu de nos jours sous son nom. Depuis, il a été utilisé comme système de cryptographie. Il employait naturellement l'alphabet grec au départ, mais je vais le décrire avec l'alphabet latin par souci de simplicité :



Le carré de Polybe. Chaque lettre (sauf J, confondu avec I) est repérée par un couple de nombres. Par exemple, M par (3, 2), ligne et colonne où se trouve M dans le carré.

Pour dessiner le carré de Polybe, on forme un carré de 5 × 5 cases que l'on remplit avec les 26 lettres de l'alphabet, sauf une. Cette lettre manquante est généralement J ou W car elles peuvent se confondre à I et V (plus précisément, I et J se confondent en latin et souvent en allemand, V et W en français mais jamais en allemand). On numérote ensuite les lignes et les colonnes. C'est ainsi que chaque lettre se voit attribuer un couple de nombres. Par exemple, M est codé par le couple (3, 2). Polybe se servait de ce chiffre pour transmettre les messages au moyen d'un jeu de torches. Ici, pour signifier la lettre M, il dirait à un soldat de brandir trois torches de son bras gauche et deux de son droit.

Le carré de Polybe permet également de chiffrer si on le complète dans un ordre différent de l'alphabet classique. Voyons cela. Le plus simple est d'employer une phrase assez longue, mais facile à retenir, comme : « depuis Vercingétorix, César et Alexandre, la discipline est la force principale des armées ». Remplissons alors le carré dans l'ordre, en supprimant les doublons, puis ajoutons les lettres manquantes :

	1	2	3	4	5
1	D	E	P	U	I
2	S	V	R	C	N
3	G	T	O	X	A
4	L	F	M	B	H
5	K	Q	W	Y	Z

Carré obtenu avec la phrase « depuis Vercingétorix, César et Alexandre, la discipline est la force principale des armées ». Pour cela, on l'écrit dans l'ordre en commençant en haut à gauche et en sautant les lettres déjà écrites. On complète ensuite par les lettres manquantes, toujours dans l'ordre.

Le chiffre de Polybe décrit ainsi est un chiffre par substitution alphabétique. Son seul avantage est de permettre une mémorisation simple de la clef. Grâce à cette propriété, le chiffre de Polybe répond à l'un des principes de Kerckhoffs, selon lequel la sécurité du système ne doit pas être assurée par le secret de son algorithme. En effet, si la clef n'a pas besoin d'être écrite, elle ne peut pas être espionnée ! Avec la clef précédente, « je vous ai compris » s'écrit : « 15 12 22 33 14 21 35 15 24 33 43 13 23 15 21 ».

Ce Qu'il Faut Décrypter

Un message philosophique

Nous avons intercepté le message suivant envoyé par un « philosophe » :

11 14 45 31 21 12 13 11 14 44 51 14 23 12 52 32 31 14 45 45 14 15 14 23 12 23 51 33 32 14 13 14 14 45 31 45 51 21 14 13 32 14 51 13 14 12 11 14 23 23 14 15 51 45 22 34 44 51 14 31 12 34 31 15 14 41 14 34 45 21 12 13 12 32 45 45 14 34 31 25 13 32 23 23 12 34 31 45 12 52 12 34 31 15 12 52 22 32 13 23 12 32 13 15 32 33 25 14 11 32 23 14 45

Sachant que notre philosophe est plutôt sarcastique et que son expression favorite est « imbécile », en trouverez-vous le sens ?

Même s'il puise ses racines dans l'Antiquité, le chiffre de Polybe est resté un classique et servait à la fin du XIX^e siècle aux nihilistes russes pour communiquer en prison ! Ces derniers formaient en effet une organisation politique qui refusait toute contrainte de la société sur l'individu. Anarchistes, ils prônaient le terrorisme et assassinèrent le tsar Alexandre II qui, pourtant, essayait de rendre son régime moins autoritaire. Le meurtre envoya un grand nombre de nihilistes derrière les barreaux. Pour échanger d'une cellule à une autre, les nihilistes frappaient sur les murs ou sur les tuyauteries de leurs prisons selon un code dérivé du carré de Polybe. Par exemple, si on utilise le carré précédent, « le tsar est mort » donne la suite de coups :

4 1 1 2 3 2 2 1 3 5 2 3 1 2 2 1 3 2 4 3 3 3 2 3 3 2.

En effet 41 signifie L, 12, E, etc.

La méthode est simple et a été sans doute employée telle quelle, mais les nihilistes la compliquaient pour rendre leur chiffre plus difficile à décrypter. Ils surchiffraient leur code à l'aide de mots-clef comme « nihil ». « Nihil » se chiffre en « 25 15 45 15 41 ». Les nihilistes répétaient cette clef sous la suite trouvée et ajoutaient les chiffres obtenus, ce qui donnait :

41 12 32 21 35 23 12 21 32 43 33 23 32

25 15 45 15 41 25 15 45 15 41 25 15 45

66 27 77 36 76 48 27 66 47 84 58 38 77

Surchiffrement du chiffre des nihilistes par un mot-clef. Si un nombre dépasse 100, on supprime le chiffre des centaines.

Avec cette méthode, « le tsar est mort » se traduit à présent par une suite de 6, 6, 2, etc. coups. Chiffrer et déchiffrer de tête ainsi exige une bonne gymnastique mentale. Un bon moyen pour conserver ses capacités intellectuelles intactes dans un environnement hostile !

Le chiffre bilitère de Francis Bacon

Le philosophe Francis Bacon (1561-1626), que certains pensent être l'auteur des pièces de Shakespeare, a inventé un chiffre entre cryptographie et stéganographie. Il est fondé sur le recours à deux façons d'écrire les lettres de l'alphabet, en romain et en italique par exemple, ce que nous noterons A et B. L'idée du carré de Polybe, avec son système de coordonnées, est sous-jacente, mais le système de Bacon exploite les polices de caractères de façon astucieuse… ce qui rend souvent le système difficile à manier. Nous le citons car certains auteurs dont Elizabeth Wells Gallup (1848-1934), tenante de la paternité baconienne des œuvres de Shakespeare, l'utilisent pour lire des messages imaginaires dans divers textes, comme nous le verrons plus loin.

	AAA	AAB	ABA	ABB	BAA	BAB	BBA	BBB
AA	a	b	c	d	e	f	g	h
AB	i	k	l	m	n	o	p	q
BA	r	s	t	u	w	x	y	z

Les 24 lettres de l'alphabet sont notées par leurs coordonnées, comme dans un carré de Polybe : ainsi, l est notée « ABABA ». On peut y voir une écriture en binaire en attribuant la valeur 0 à A et la valeur 1 à B, mais, sans preuve supplémentaire, il serait imprudent de faire de Bacon un

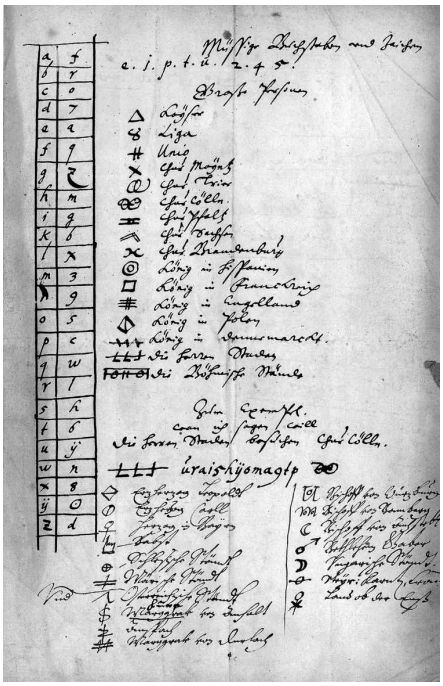
précurseur du système binaire. On choisit alors un texte dont le sens importe peu car le message est dans la typographie. Si A désigne le romain et B l'italique, le message « rendez-vous à cinq heures à la Bastille » ayant 32 caractères se chiffre d'abord en : BAAAA AABAA ABBAA AAABB AABAA BABBB BAABB ABBAB BAABB BAAAB AAAAA AAABA ABAAA ABBAA ABBBB AABBB AABAA BAABB BAAAA AABAA BAAAB AAAAA ABABA AAAAA AAAAB AAAAA BAAAB BAABA ABAAA ABABA ABABA AABAA On choisit alors un texte ayant au moins le même nombre de caractères, par exemple le début du poème « Le pont Mirabeau » de Guillaume Apollinaire, en écrivant les lettres soit en romain, soit en italique, pour faire passer le message :

*S*ous le p*o*nt M*ir*abeau *co*ul*e* la *Se**i**ne E*t nos a*mo*u*rs*
Fa*ut-i*l qu'*i*l m'en souv*ie*n*n*e La j*oi*e ve*nait* to*ujo*ur*s* ap*r*ès *la p*eine.
Vi*enn**e* la n*u*it sonn*e* l'*h*eure Les jou*r*s s'en v*o*nt j*e d*eme*u*r*e*.
Les m*ain*s d*an**s* les *m*ains, restons face à face.

Par exemple, les cinq premières lettres (« *S*ous l ») véhiculent le code « BAAAA » (B pour italique et A pour romain) qui signifie « r » et ainsi de suite.

Nulle, mais mieux !

Comme vous avez pu le constater vous-même depuis le début du chapitre, aucun besoin d'avoir le QI d'Einstein pour décrypter des chiffres par substitution. Au fil des siècles, même si les cryptologues continuaient à y recourir, on prit conscience de la faiblesse de ces codes et on chercha à les améliorer en les « bricolant ». Un premier essai fut d'introduire au sein des substitutions ordinaires des symboles ne signifiant rien, des « nulles » dans le langage des cryptologues. Un autre ajout consista en un nomenclateur pour désigner les personnages importants. Voici un exemple de l'un de ces chiffres perfectionnés datant de 1619-1620, toujours conservé dans les archives de la ville de Strasbourg (voir p. suivante).



Cette table de chiffrement, conservée aux archives de Strasbourg, est datée de 1619-1620. Elle contient un alphabet chiffré (à gauche), des nulles (en haut) un nomenclateur (à droite) et un exemple (au milieu). Le tout est écrit en allemand dans le graphisme d'époque.

Même s'il s'agit toujours d'un chiffre par substitution alphabétique simple, cette table de chiffrement est particulièrement intéressante car elle introduit des nulles (e, j, p, t, u, 2, 4, 5) en plus d'un nomenclateur pour des personnes importantes comme des princes-électeurs, des évêques et des rois. De plus, cette table contient un exemple, « urai5hyomagtp » qui, une fois les nulles supprimées, devient « rahyomag », qui se déchiffre au moyen de l'alphabet inversé en « besuchen ».

Hélas pour ses promoteurs, cette tentative d'amélioration était insuffisante. Quelle que soit la méthode de substitution mono-alphabétique employée, elle est cassable par une analyse des fréquences et la méthode du mot probable. Que faire alors ? L'idée la plus simple, pour contourner ces méthodes de décryptement, est de proposer plusieurs chiffrements des lettres les plus courantes comme E, A, etc. Bien sûr, ce n'est pas possible avec des lettres, mais cela le

devient avec des nombres ou des symboles, comme ceux des Templiers. Toutefois, c'est une fausse bonne idée, car de tels chiffres qui ont été utilisés à la Renaissance s'écroulent devant la technique du mot probable.

À l'époque, un détail facilitait en outre le travail des décrypteurs : les missives d'intérêt majeur étaient souvent envoyées en multiples exemplaires jusqu'à réception d'une réponse. Cela peut sembler une broutille, mais par ce biais apparaissaient des équivalences qui fourniront des indices. Prenons un exemple. Supposons que nous interceptions les deux messages ayant le même expéditeur et le même destinataire :

> Vx kεosyrmmx fx yrnlγ ex ajγluffx ex ljβdδkrm Vγ krosyεmmγ fx yεnlγ ex ajxluffx eγ ljzdukrm

Le nombre de lettres, le découpage des mots et l'importante identité des lettres suggèrent qu'il s'agit du même message, chiffré différemment. On peut ainsi en déduire les équivalences : x = γ, r = ε, u = δ et z = β. Un décompte des signes x et γ montre que ces deux symboles représentent probablement la lettre E, et le message partiellement décrypté devient :

> V**E** k**E**osy**E**mmx fx yrnl**E** e**E** aj**E**luff**E** e**E** ljzdukrm

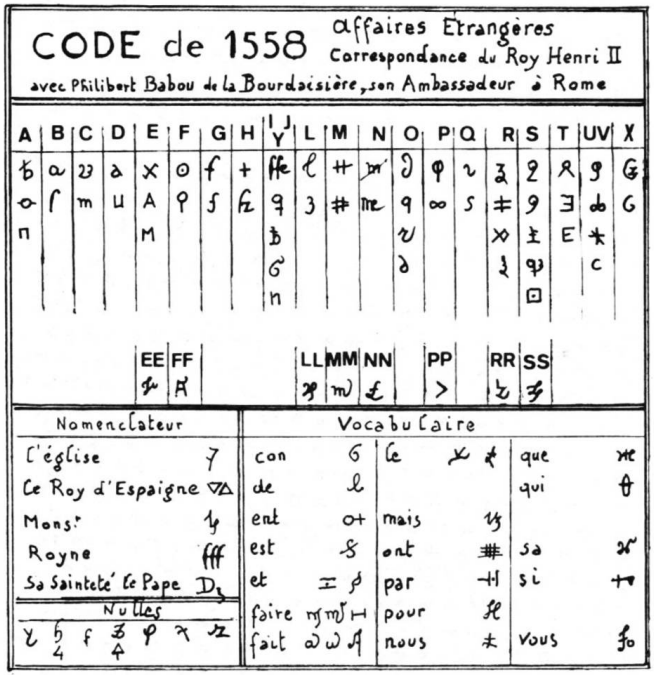
Le texte est trop court pour aller plus loin sans mot probable, mais on voit que l'avantage de l'homophonie est vite perdu si plusieurs missives chiffrant le même texte de façons différentes sont interceptées. C'est une faille qu'avait exploitée notamment François Viète pour décrypter les dépêches de Philippe II.

À la cour de François I^{er}

Ces chiffres homophoniques furent malgré tout privilégiés à la Renaissance, où on les associait à un nomenclateur – un très court dictionnaire chiffré. Les symboles étaient de style « cabalistique », même si cela ne servait à rien. À titre d'exemple, je vous propose de nous pencher sur une table de

chiffrement authentique des archives de Strasbourg, puis sur une table reconstituée concernant le roi Henri II.

La table de chiffrement ci-contre est typique de la Renaissance. Ce chiffre est du niveau de ceux des rois de l'époque. C'est ce que montre le chiffre de Philibert Babou de la Bourdaisière fils ci-dessous. Son père, qui portait le même nom, fut surintendant des finances du roi François Ier et, partant, son cryptanalyste.



Reconstitution du code de Philibert Babou de la Bourdaisière fils. Il s'agit d'un chiffre par substitution, auquel on a ajouté plusieurs équivalences pour chaque lettre et un court nomenclateur.

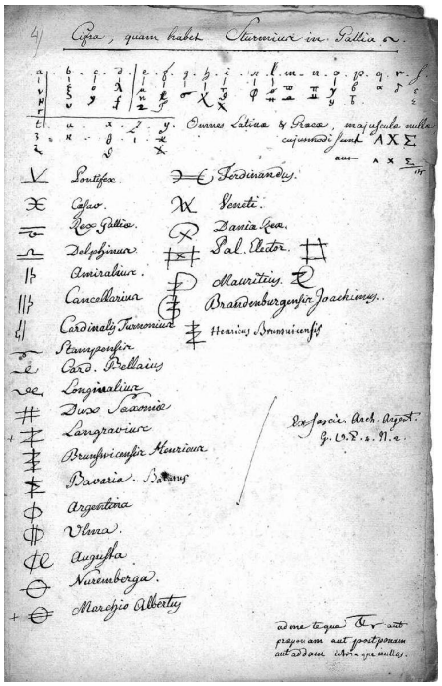


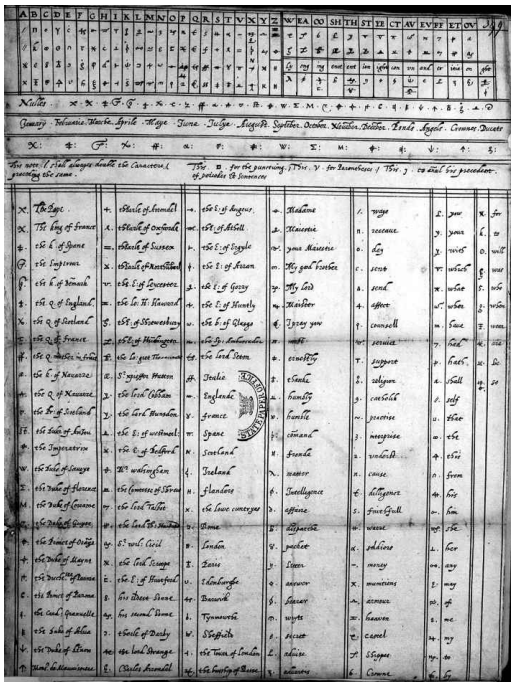
Table de chiffrement multiple avec nulles et nomenclateur plus un symbole en bas à droite, destiné à annuler une partie du texte. L'existence de ce type d'instructions explique la difficulté qu'on peut avoir à déchiffrer, même en connaissant la table. Le lecteur intéressé par l'histoire de l'Alsace décryptera l'inscription latine en tête de la table et y trouvera un personnage célèbre au niveau local : Jean Sturm, dont un lycée de Strasbourg (le gymnase) porte le nom.

La petite histoire raconte que le père passait tellement de temps à décrypter les messages interceptés par les services du roi qu'il délaissait son épouse. Bon prince, le roi remplissait son devoir conjugal à sa place… Nous disposons du chiffre du fils, cardinal et ambassadeur du roi Henri II à Rome.

Ces chiffres restaient faibles, malgré l'invention des nulles et même l'ultime perversité d'y inclure des symboles annulant le symbole suivant ou le précédent. Ils s'écroulaient en effet dès qu'un nombre suffisant d'équivalences était découvert. En revanche, la méthode des fréquences ne sert à rien pour les attaquer. Mieux vaut privilégier celle du mot probable. Les deux chiffres historiques suivants ont été cassés de cette façon.

Le chiffre de Marie Stuart

Ayant été élevée à la cour de France à l'époque d'Henri II, il est logique que Marie Stuart, reine d'Écosse devenue reine de France, ait privilégié un chiffre du type de celui de Philibert Babou fils. Elle en employait même plusieurs, en fonction de ses correspondants. Or ses chiffres lui firent perdre la tête, littéralement.



Chiffre de Marie Stuart. Comme il était courant à son époque, il comportait de multiples correspondances pour les lettres, des chiffres particuliers pour les digrammes courants de l'anglais et un nomenclateur.

Son sort se joua alors qu'elle était prisonnière au château de Chartley, dans le nord de l'Angleterre. Son seul contact avec le monde extérieur se faisait via des lettres chiffrées par son secrétaire et sorties clandestinement, cachées dans des tonneaux de bière. Or la personne chargée de cette tâche s'avéra être un agent double, au service de la reine d'Angleterre Élisabeth I^er^. Les lettres furent transmises au

cryptanalyste Thomas Phelippes, qui les décrypta vraisemblablement avec la méthode des mots probables. L'abondance des messages lui facilita certainement la tâche.

Un beau jour de 1586, Marie Stuart reçut une lettre où son ancien page (le noble sous ses ordres) lui annonçait qu'un complot se préparait contre la reine d'Angleterre et lui demandait son accord. La réponse de Marie scella son destin. En plus d'être un bon décrypteur, Thomas Phelippes était aussi un faussaire hors pair. Quand il eut décrypté la lettre de Marie, il la recopia et y ajouta un post-scriptum demandant au destinataire les noms de tous les comploteurs. Ainsi, le page livra lui-même ses complices, qui furent tous exécutés.

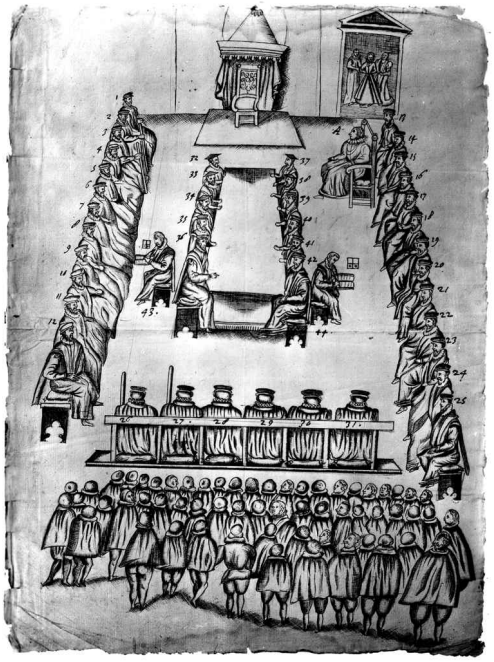
Ce Qu'il Faut Décrypter

Un message d'Henri à Claire

Henri envoie le message suivant à Claire :

Di2sf dm1js 2sfoe faw4v tdft4 js1mi f5sfi 1cju5 fmm2q mbd2e fm1cb tu3mm fi2os j

Savoir qu'Henri commence toujours ses messages par « chère Claire » et signe à la fin de son nom vous suffira-t-il pour le décrypter ?



Le procès de Marie Stuart (*A*, en haut à droite) en octobre 1586. La reine fut trahie par son système de chiffrement trop faible, comme tous ceux de l'époque.

Le défi du tueur du zodiaque

Malgré leur faiblesse (et la mort de Marie Stuart), les chiffres homophoniques ne furent pas remisés au placard. Au XX^e^ siècle, ils firent même la une des journaux sous la plume… d'un serial killer. Le tueur du zodiaque sévissait en Californie à la fin des années 1960. Tout porte à penser qu'il est mort depuis, puisque ses crimes et ses revendications ont cessé, mais rien ne le prouve, car il n'a jamais été arrêté. Pensant certainement faire étalage de son intelligence, il envoya plusieurs messages chiffrés à la police et à la presse.

Début d'un message chiffré envoyé par le tueur du zodiaque.

Dans un texte accompagnant le premier message, le Zodiaque demandait la publication de celui-ci (et une lettre où il revendiquait certains meurtres) en première page des journaux, menaçant de se livrer à de nouveaux meurtres si son exigence n'était pas respectée. Finalement, le *San Francisco Examiner* publia la lettre à la page quatre.

Le message semblait être codé par le biais d'une méthode par substitution. Il fut décrypté par un enseignant et son épouse, Donald et Betty Harden. Leur idée fut d'entrer dans la psychologie d'un tueur en série qui, selon eux, devait posséder un ego surdéveloppé. Pour eux, le message devait commencer par la lettre « I » qui, en anglais, signifie « Je ». Ensuite, le couple chercha les mots « kill » et « killing » (« tuer »). Le code s'écroula ensuite petit à petit. Pour tromper les décrypteurs, le tueur avait de plus effectué de nombreuses fautes d'orthographe. Voici le message décrypté :

I LIKE KILLING PEOPLE BECAUSE IT IS SO MUCH FUN IT IS MORE FUN THAN KILLING WILD GAME IN THE FORREST BECAUSE MAN IS THE MOST DANGEROUS ANAMAL OF ALL TO KILL SOMETHING GIVES ME THE MOST THRILLING EXPERENCE IT IS EVEN BETTER THAN GETTING YOUR ROCKS OFF WITH A GIRL THE BEST PART OF IT IS THAT WHEN I DIE I WILL BE REBORN IN PARADICE AND ALL THE I HAVE KILLED WILL BECOME MY SLAVES I WILL NOT GIVE YOU MY NAME BECAUSE YOU WILL TRY TO SLOI DOWN OR STOP MY COLLECTING OF SLAVES FOR MY AFTERLIFE EBEORIETEMETHHPITI

Nous pouvons le traduire ainsi :

J'aime tuer les gens parce que cela me fait plaisir, plus que de tuer du gibier dans la forêt, parce que l'homme est l'animal le plus dangereux de tous à tuer. C'est excitant, même plus que d'avoir du bon temps avec une fille. Le mieux sera quand je mourrai. Je renaîtrai au paradis et tous ceux que j'ai tués deviendront mes esclaves. Je ne donnerai pas mon nom car vous essayeriez de ralentir ou de stopper ma récolte d'esclaves pour mon au-delà. Ebeorietemethhpiti.

Sa signature restera incompréhensible…

Un individu, sans doute psychopathe, nommé l'entarteur masqué a envoyé le message suivant à la presse :
LPΞΠG MΣXQΣ Φ8QNΩ IJ8ΔΓ XΞLGQ ΞEΞW8 ΠΞIΦQ ΠΔIVQ GΣΔMΣ ΞG8YJ 8ΞMP8 ISP89 ΦQMGM ΣP8IΔ RPMΣΩ VVΦΠG QVΞVP ΠΔIΠΦ IVΞVP ΠΔIWG IΣE8V ΞVGX8 9Ξ9GΠ ΔIΣΩQ ΣΦI
L'hypothèse qu'il commence par : « Moi, l'entarteur masqué… » vous suffira-t-elle pour le décrypter ?

Le chiffre des émigrés

Dans la catégorie des chiffres homophoniques que nous explorons depuis la moitié de ce chapitre figure également celui employé en 1793 par l'armée des émigrés. Il s'agissait d'un groupe contre-révolutionnaire composé de nobles ayant fui la France et qui complotaient de l'étranger pour rétablir la monarchie. Pour chiffrer leurs communications, ses membres se servaient d'une version complexifiée du chiffre de César. Le décalage transformait A en D, B en E, etc. En outre, des chiffres codaient les voyelles, à savoir 38, 39, 40 et 41 pour A, 22, 23, 24 et 25 pour E, 26, 27, 28 et 29 pour I, 30, 31, 32 et 33 pour O, 34, 35, 36 et 37 pour U. À cela s'ajoutaient des digrammes pour certains mots, de « aa » pour Anjou jusqu'à « bn » pour Woronzoff en passant par « ab » pour argent et « ai » pour émigrés. Malgré ces amendements, ce chiffre n'était guère plus solide que celui des correspondances personnelles du *Figaro…*

Le chiffre de Playfair

Afin de rendre la méthode des fréquences plus difficile à appliquer, le physicien et inventeur anglais Charles Wheatstone (1802-1875), plus connu pour le montage électrique qu'il inventa pour mesurer précisément les résistances électriques, eut l'idée de construire un chiffre de substitution en échangeant non plus des lettres avec des

lettres, mais des digrammes avec des digrammes. En effet, si les lettres sont au nombre de 26, les digrammes (de AA à ZZ) sont au nombre de 26 fois 26, c'est-à-dire 676 ; pour distinguer un symbole parmi 676 grâce à l'analyse des fréquences, il faut pouvoir traiter des centaines de messages. L'inconvénient de la méthode ? La nécessité de retenir un livre conséquent de codes. Pour faciliter cette étape, Wheatstone proposa de détourner le carré de Polybe de son utilisation première. Wheatstone était anglais, mais optons pour un poème français déjà cité pour illustrer sa méthode :

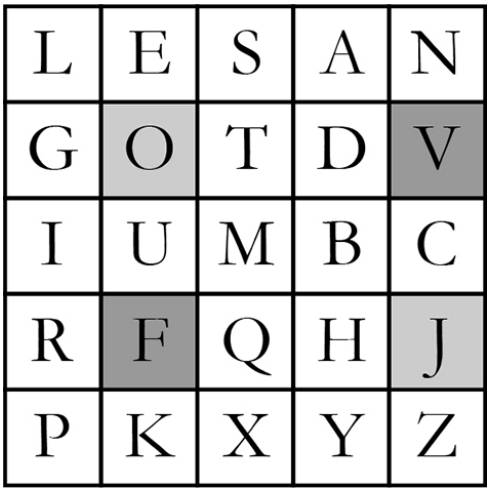
Les sanglots longs des violons de l'automne
Blessent mon cœur d'une langueur monotone.
Tout suffocant et blême, quand sonne l'heure,
Je me souviens des jours anciens et je pleure,
Et je m'en vais au vent mauvais qui m'emporte Deçà, delà pareil à la feuille morte.

Remplissons le carré comme déjà vu, en évitant les doublons.

L	E	S	A	N
G	O	T	D	V
I	U	M	B	C
R	F	Q	H	J
P	K	X	Y	Z

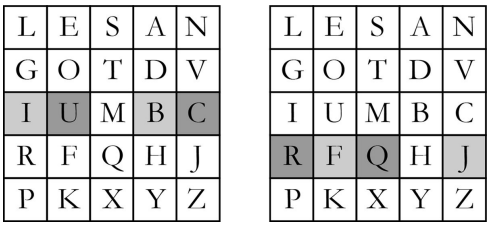
On remplit le carré avec la poésie donnée, puis on complète par les lettres manquantes (le W est confondu avec le V).

Ce carré permet de chiffrer les digrammes par d'autres digrammes. Le cas général est simple et très géométrique, puisqu'il consiste à construire un rectangle dans le carré.



Pour chiffrer le digramme OJ, on construit le rectangle dont les sommets opposés correspondent à O et J. Les deux autres sommets (dans le même ordre) donnent le code VF (dans l'ordre des lignes de O et J).

L'inconvénient est que cet algorithme de substitution comporte trois cas particuliers ! Premièrement, on peut avoir affaire à deux fois la même lettre. La convention est alors d'intercaler une lettre convenue d'avance, souvent X. Dans le cas peu probable où le digramme est XX, on intercale une autre lettre, Y par exemple. On chiffre alors les nouveaux digrammes. Les autres cas particuliers sont les cas où les lettres sont sur la même ligne ou la même colonne. La règle est encore géométrique et elle s'adapte au cas des colonnes.



Si les lettres sont sur une même ligne, on les remplace par celles qui les suivent sur la ligne (dans l'ordre). Ainsi, IB devient UC. Si la seconde est en dernière colonne, on la remplace par celle en première colonne.

Imbéciles d'ambassades

Wheatstone présenta ce chiffre au ministère des Affaires étrangères britannique, qui le refusa car il le trouvait… trop complexe. Le scientifique aurait alors proposé de montrer que son système pouvait être maîtrisé en moins de quinze minutes par les trois quarts des garçons de l'école voisine. À quoi le sous-secrétaire du ministère aurait répondu : « C'est possible, mais vous n'arriverez pas à l'apprendre à des attachés d'ambassade. » Difficile de savoir si cette histoire est vraie, même si on doit reconnaître que ce chiffre est d'un emploi délicat. Un ami de Wheatstone, lord Lyon Playfair, réussit toutefois à le faire accepter par les autorités militaires, d'où le nom sous lequel le chiffre est désigné de nos jours.

Le chiffre de Playfair fut déployé par les Britanniques en 1914. Le cryptologue américain Joseph Mauborgne (1881-1971) montra la même année comment le décrypter et, de fait, les Allemands y parvenaient en quelques heures. Les Britanniques ne l'employèrent donc que pour protéger des informations demandant un secret de courte durée, comme l'annonce d'un tir de barrage pour couvrir une avance vers les lignes ennemies.

Avant que je vous expose comment le casser, voyons comment les Britanniques s'y prenaient pour déchiffrer des messages codés avec. Pour cela, imaginons que nous recevions le message chiffré suivant :

XGUNS VLSFK UVIEA OSOFG MGIAN BEOMS DVOFS QRGES TSETU SFLEM SFMUY LOLVT CKAOS UNLOA CLKUQ ISDUG SZ

Pour le déchiffrer, on applique les règles précédentes à l'envers. On commence donc par le couple XG, qui donne PT (voir le carré précédent). De même, UN donne CE, etc. La signification apparaît à la fin de notre déchiffrement : « PT 109 coulé. Détroit Blackett. Deux milles Sud-Ouest Meresu. Équipage 12. Demande information. »

Un chiffre Playfair connu

Quand la nuit sur le front dont il s'occupe est calme, le général Sanche envoie le message suivant au petit matin : « Nuit calme sur le front est de Nancy. Général Sanche. » Au petit matin, on intercepte le message chiffré :

FPDSN LERTM PMETC UAFOT ISKTH PCBVJ ABLML EPTCB KA

puis le message :

LOOLV STLQD AXOMM LPQUP CRLNA OLBAB OQFCD OFLEA BAAJL PJQ

Pouvez-vous le décrypter ?

Ce message fait référence à un événement historique lié au futur président des États-Unis, John Kennedy, alors qu'il était officier de marine pendant la Seconde Guerre mondiale. Il commandait un patrouilleur (le *PT 109*) en 1943 quand son bateau fut éperonné et coupé en deux par un destroyer japonais. Avec les survivants, il réussit à s'agripper à la proue pour finalement rejoindre une île déserte à la nage. Au moyen de la radio de bord, qu'il avait conservée, Kennedy envoya alors le message suivant, version anglaise de celui donné plus haut.

KXJEY UREBE ZWEHE WRYTU HEYFS KREHE GOYFI WTTTU OLKSY CAJPO BOTEI ZONTX BYBWT GONEY CUZWR GDSON SXBOU YWRHE BAAHY USEDQ

Les garde-côtes australiens utilisaient couramment le chiffre Playfair, ce que savait John Kennedy. Ce dernier connaissait visiblement les clefs courantes, puisque les Australiens déchiffrèrent son message : il fut secouru dix heures plus tard. Un film a romancé l'histoire depuis, de façon très éloignée de la réalité – le message se trouve gravé sur une noix de coco et transporté par des indigènes. Le code a sans doute été jugé trop compliqué pour le public…

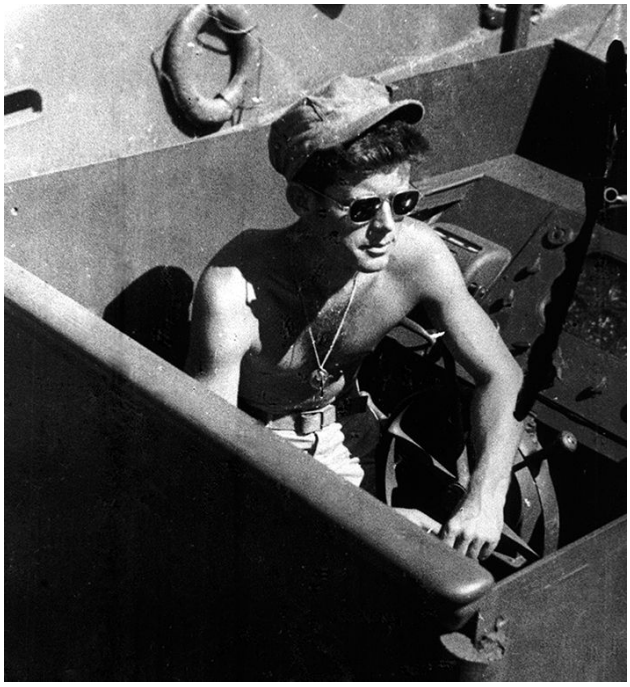
Le message de Kennedy

Voici le message du futur président :

KXJEY UREBE ZWEHE WRYTU HEYFS KREHE GOYFI WTTTU OLKSY CAJPO BOTEI ZONTX BYBWT GONEY CUZWR GDSON SXBOU YWRHE BAAHY USEDQ

La clef servant à chiffrer son message était « Royal New Zealand Navy ».
Saurez-vous porter secours au naufragé ?

Les Japonais n'étaient pas loin, mais, heureusement pour Kennedy et son équipage, ils furent incapables de décrypter son message. C'était pourtant possible grâce à l'analyse des fréquences des digrammes. Les plus courants en français sont ES, EN, ON, OU, TE, NT et DE.



Le futur président des États-Unis, John Kennedy, à bord du patrouilleur *PT 109* en 1943.

Le chiffre de Hill, ou l'irruption des maths

Le chiffre de Playfair invitait à une généralisation aux trigrammes, tétragrammes et au-delà, de façon générale aux polygrammes. Après plusieurs échecs empruntant la voie géométrique de Wheatstone, un mathématicien américain, Lester Hill (1891-1961), reprit la question en s'appuyant sur l'algèbre et l'arithmétique modulaire. Ce mot compliqué de « modulaire » recouvre en fait une réalité simple. Les lettres de l'alphabet latin peuvent être remplacées de plusieurs façons par des nombres, soit dans l'ordre, soit dans le désordre. Par exemple, on peut convenir de la correspondance suivante, où les nombres sont pris entre 0 et 25 :

A	B	C	D	E	F	G	H	I	J	K	L	M
15	**7**	**2**	**14**	**23**	**9**	**25**	**21**	**13**	**8**	**16**	**11**	**1**

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
3	**10**	**24**	**12**	**5**	**4**	**0**	**18**	**20**	**19**	**22**	**17**	**6**

Ce tableau permet de coder tout digramme par un couple de nombres entre 0 et 25. Ainsi, EN et (23, 3) peuvent être considérés comme la même entité. Le chiffrement des digrammes s'opère alors par le calcul et non par la géométrie, comme dans le chiffre de Playfair. La clef est constituée de quatre lettres correspondant à quatre nombres a, b, c, d. Le chiffré d'un digramme (u, v) est alors le digramme (x, y) où x et y sont donnés par les deux équations :

$x = a\,u + b\,v$ et $y = c\,u + d\,v$

sachant que les opérations s'opèrent modulo 26, c'est-à-dire que leurs résultats sont systématiquement remplacés par leurs restes dans la division par 26.

Si la clef est RFZH, soit (5, 9, 6, 21), le chiffré de EN (23, 3) correspond aux calculs : x =5.23 + 9.3 = 142 soit 12 modulo

26, soit Q et $y = 6.23+ 21.3 = 201$ soit 19 modulo 26, soit W. Le chiffré du digramme EN est donc QW. Pour déchiffrer, il est nécessaire de calculer u et v en fonction de x et y. Le calcul apporte une surprise : le chiffré de QW est EN, comme le montrent les calculs : $5.12 + 9.19 = 231$ soit 23 modulo 26, soit E et $6.12 + 21.19 = 471$ soit 3 modulo 26, soit N.

Ce résultat est général mais correspond à notre choix particulier de clef. On déchiffre comme on chiffre. Nous avons déjà rencontré cette particularité avec le Rot13 et les alphabets réversibles. Quand chiffrement et déchiffrement se confondent, on parle de chiffrement involutif, en empruntant le vocabulaire des mathématiques, où une fonction est dite involutive si elle est sa propre réciproque. Dans le cas du chiffrement de Hill, cette contrainte d'involutivité laisse un grand nombre de choix de clefs possibles.

La méthode s'étend aux trigrammes, tétragrammes, etc. Le chiffre de Hill lie donc la cryptographie aux mathématiques et ouvre la voie à l'utilisation de groupes et de corps finis, comme dans le système RSA ou les courbes elliptiques, que nous verrons plus loin (voir le chapitre 13). Ici, l'un des défauts du chiffre que nous avons proposé est l'utilisation du nombre 26, car l'ensemble des nombres entre 0 et 25 muni de l'addition et de la multiplication modulo 26 n'a pas les propriétés algébriques des nombres réels. C'est ainsi que certains nombres non nuls ne sont pas inversibles, puisque $2.13 = 0$ modulo 26.

Pour pallier ce type de problème, il vaut mieux remplacer 26 par un nombre premier, 29 par exemple, en ajoutant quelques symboles additionnels aux lettres de l'alphabet. Nous verrons plus loin cette irruption des nombres premiers en cryptographie avec la méthode RSA. De ce point de vue, le chiffre de Hill a un intérêt plus théorique que pratique, du fait de sa lourdeur. Mais il a le mérite de lier fermement la cryptographie aux mathématiques. C'est grâce à ce lien que de nombreux mathématiciens se sont vu proposer un poste

dans les services du chiffre au cours de la Seconde Guerre mondiale.

Ce Qu'il Faut Décrypter

Un chiffre affine

On intercepte le message :

MFXEF SORUF DIMRH HRORH LADUU ERHFU UDSRH RHKOR SRKER BNROR HLADU UERHY FEHNI HKDKN KDVSL RPRHH FXRRH KOVSL UFLDM RFORL EZYKR E

On sait qu'il a été chiffré par un chiffrement affine, c'est-à-dire que chaque lettre est d'abord convertie en un nombre x entre 0 et 25, puis remplacée par le reste dans la division par 26 du nombre a x + b où a et b sont deux nombres… qui est ensuite convertie en lettre avec la conversion du départ.

Ces éléments vous suffiront-ils pour le décrypter ?

5 La révolution de Rossignol et la pincée de désordre

Au-delà des considérations autour de sa sécurité, la complexité d'une méthode de chiffrement est un point clef. Or, si chiffrer les digrammes était une bonne réponse à la faiblesse des chiffres par substitution mono-alphabétique, la difficulté rebuta sans doute les cryptologues. Non : la véritable invention qui fit faire un bond en avant à la cryptographie et rendit les chiffres plus sûrs est venue d'Antoine Rossignol, le fondateur du Cabinet noir que nous avons déjà rencontré au début de ce livre. Rossignol fut à l'origine des dictionnaires chiffrés désordonnés, dont l'un des meilleurs exemples a été le Grand Chiffre de Louis XIV. Avec succès puisque, telle une forteresse imprenable, le Grand Chiffre a résisté trois siècles aux assauts des décrypteurs !

Un chaînon intermédiaire

Les tables de chiffrement rencontrées jusqu'ici correspondent à des substitutions alphabétiques, éventuellement pourvues de nomenclateurs. Pourtant, comme nous l'avons vu aux premiers chapitres, le début du XX^{e} siècle sera marqué par l'utilisation de dictionnaires chiffrés (rappelez-vous, il s'agit d'une longue litanie de

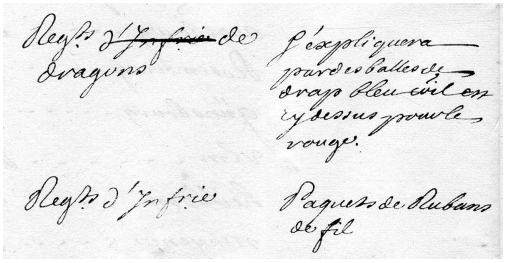
correspondances entre des nombres et des mots). Comment s'est effectuée la transition des unes aux autres ? Dans les archives de Strasbourg toujours, la première table ressemblant à un dictionnaire chiffré est datée de 1636. Elle servait à la correspondance entre le souverain de Bavière et son général en chef sur le terrain (le feld-maréchal Goetz, pour les passionnés d'histoire). Il s'agit d'une sorte d'intermédiaire entre les chiffres homophones et les dictionnaires chiffrés désordonnés. Les chiffres n'y sont d'ailleurs pas des nombres, comme c'est le cas dans les dictionnaires chiffrés, mais des symboles suivis de nombres.

Proto-dictionnaire chiffré des archives de Strasbourg, daté de 1636 (détail).

L'avantage de cette méthode ? C'est tout simplement de permettre un déchiffrement facile à l'aide de la seule table de chiffrement. Hélas, son inconvénient majeur est que les chiffres des mots commençant par la même lettre sont ordonnés entre eux… Je m'explique : si on découvre que 910 signifie *ab* et 920 *alb*, alors les chiffres entre 911 et 919 correspondent à des mots entre *ab* et *alb* dans l'ordre alphabétique. Conscient de cette faiblesse (qui devient une faille entre les mains d'un décrypteur), le grand Antoine Rossignol fut le premier à modifier ces tables et à élaborer des dictionnaires chiffrés désordonnés, ce qui conduisit au

Grand Chiffre. En outre, par prudence, Rossignol faisait toujours garder un chiffre neuf en réserve sous pli cacheté. Ainsi, si on s'apercevait qu'un chiffre n'était plus secret, on pouvait en changer immédiatement (ces problèmes de logistique liés au partage du secret sont d'ailleurs toujours d'actualité).

Il semble que la faiblesse soulignée par Antoine Rossignol soit généralisée dans la première moitié du XVIIe siècle. Elle se retrouve, tout ou partie, dans un certain nombre de chiffres datés du règne de Louis XIV, où tous les mots commençant par a ou b sont chiffrés dans l'ordre par des nombres finissant par 1, de même pour les mots commençant par « da » avec un nombre finissant par 2, etc. Ces chiffres sont accompagnés d'une liste de termes servant à camoufler des noms propres (personnalités, lieux et matériels). Ainsi les « oranges » sont des « bombes » et les « citrons », des « grenades », la « forêt noire », « zurzach », etc. De façon générale, les noms des villes sont échangés.



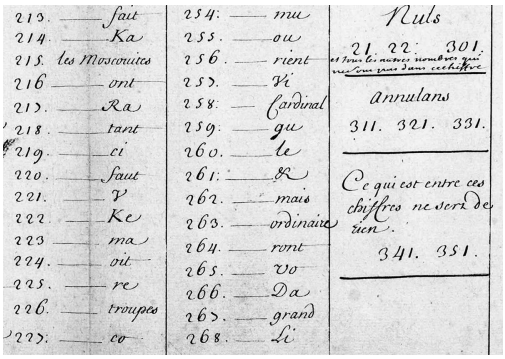
Instruction pour donner le nombre de régiments de dragons et d'infanterie (devenus des « paquets de rubans de fil »…).

Table de chiffrement pour la correspondance entre le marquis d'Huxelles et le marquis de Villard. Les chiffres y sont désordonnés et des instructions de nullité sont là pour compliquer la tâche des décrypteurs. Ainsi, on voit dans l'avant-dernière colonne qu'en plus des nuls et des annulants (le chiffre suivant), deux symboles servent à entourer des parties entièrement nulles.

Du chaos naît la sûreté

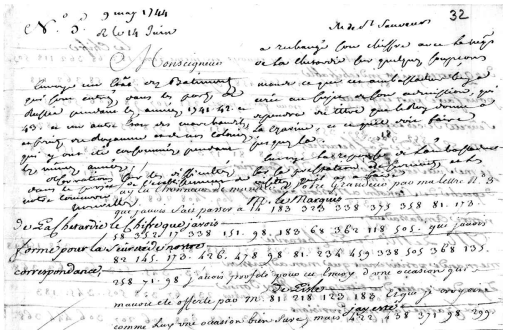
Pour être véritablement solides, ces dictionnaires chiffrés doivent être désordonnés. À partir des années 1680, la plupart des chiffres se trouvant dans les archives de Strasbourg le sont, comme celui servant à la correspondance entre le marquis d'Huxelles et le marquis de Villard.

Pour déchiffrer, on ne peut plus se contenter de lire les tables de chiffrement à l'envers, ce qui reviendrait à utiliser un dictionnaire français/allemand pour traduire un texte allemand en français. La recherche des mots serait extrêmement fastidieuse ! Pour faciliter le travail de traduction chiffres/mots, des tables de déchiffrement sont apparues, ordonnées selon les chiffres. Dans la table ci-dessous, on voit ainsi rapidement que « 258 » signifie « Cardinal ».



Extrait d'une table de déchiffrement pour la correspondance entre le marquis d'Huxelles et le marquis de Villard.

À l'époque, l'usage était de déchiffrer directement sur le message, comme l'illustre l'extrait ci-dessous d'une lettre venant de Saint-Pétersbourg et reçue par le secrétaire de la Marine, le comte de Maurepas, en 1744. On notera que la missive n'est chiffrée que partiellement, ce qui est une faiblesse puisqu'elle risque d'offrir une foule de mots probables.



Extrait d'une lettre partiellement chiffrée, datée de 1744. Envoyée depuis Saint-Pétersbourg, elle était destinée au comte de Maurepas.

Ces tables étaient accompagnées d'instructions pour les utiliser. Voici le début de celles liées à la table de Puisieulx de 1750. Destinée à la diplomatie française, elle contenait 12 000 nombres…

> Vous trouverez, Monsieur, dans ce paquet trois nouvelles tables de chiffre, savoir un ordinaire, un de réserve et un de correspondance avec une instruction sur la manière de s'en servir. Vous sentirez aisément combien il importe que vous recommandiez à vos secrétaires de se conformer scrupuleusement à cette instruction.

Nous voyons immédiatement qu'une table de réserve était prévue, précaution que prenait déjà Rossignol. Un certain nombre de règles impératives suivent, dont la première est :

> Il ne faut absolument mettre dans les articles chiffrés aucun mot en clair, et être très attentif que le chiffre ne paraisse avoir aucune raison avec ce qui le précède ou ce qui le suit en clair, et que ce qui précède ou ce qui suit ne puisse fournir aucune lumière sur les articles chiffrés. […]
> En commençant la dépêche ou l'article qui doit être chiffré après avoir mis dans la première ligne 6 ou 7 nombres pris au hasard, on chiffrera ce qui doit l'être jusqu'à la fin ; alors on se servira du nombre qui marque la fin et on mettra ensuite quelques nombres pris au hasard […]
> On ne se servira du chiffre de réserve que lorsque l'on aura lieu de soupçonner que le chiffre ordinaire n'est plus sûr. Alors on ne se servira en aucun cas du chiffre ordinaire et les dépêches seront chiffrées du chiffre de réserve.

Ce dernier point est destiné à éviter d'offrir à un éventuel intercepteur du chiffre ordinaire une pierre de Rosette, lui permettant de découvrir le chiffre de réserve.

La régression de la Révolution et de l'Empire

L'excellence française en matière de cryptographie se termina à la Révolution. Une des raisons est sans doute la dissolution du Cabinet noir, ce qui était une des doléances importantes de 1789. Une expertise qui se transmettait de génération en génération semble alors s'être perdue. En particulier, la faiblesse de ne chiffrer que les parties qu'on veut garder secrètes devint presque systématique dans l'armée révolutionnaire comme dans l'armée impériale qui lui succéda. On y distinguait deux types de chiffres, les petits et les grands (les grands étant censés être plus solides que les petits), même s'il ne serait pas exagéré de

dire qu'ils étaient tous rendus petits par leurs utilisateurs, comme cela ressort de l'examen des papiers de George Scovell (1774-1861), le décrypteur du général britannique Wellington (le vainqueur de Waterloo).

Comme ils le feront ensuite au cours des deux guerres mondiales, les Britanniques systématisèrent l'interception et le décryptement des messages en créant, sous les ordres de Scovell, un corps d'éclaireurs. Ces derniers étaient chargés, en plus de la mission habituelle de guider l'armée, de porter les messages, d'intercepter ceux de l'ennemi, mais aussi de les décrypter. Ces éclaireurs étaient choisis pour leur connaissance du français, de l'espagnol et de l'anglais, au-delà de leurs qualités proprement militaires. Rappelons qu'au début du XIXe siècle, l'Europe de l'Ouest était déchirée par une guerre opposant la France aux forces alliées réunissant la plupart des autres pays, dont la Couronne d'Angleterre, l'Allemagne et l'Espagne.

Ce Qu'il Faut Décrypter

Le message du commandant Pulier

En 1796, pendant la campagne d'Italie, alors qu'il se trouve en Ligurie, le commandant Pulier envoie à son général le message suivant, conservé dans les Archives de l'armée :

10000 20414 13120 70002 03001 91317 00190 00705 11201 40011
00201 40521 04072 30300 01001 60521 05031 11104 19090 01707
00190 50903 00071 30507 00241 41104 07090 70009 00130 00700
19090 70009 00010 50319 05060 31905 11000 50319 13032 01400
11001 20700 01030 00716 05210 50311 11041 90900 24250 51313
00140 71309 00110 31719 00201 40403 20140 01100 09002 10524
25000 10019 21201 40300 21050 32105 13120 42104 07190 41900
13040 32112 05130 90001 05090 30203 13030 41910 00110 50324
00120 01909 05192 10605 03210 70011 00020 00712 05070 10013
21070 41412 00131 00002 04141 31207 03000 90009 04191 90007
09001 30407 09070 01312 04140 71100 07000 11211 05240 00100
19210 90024 00090 02105 24250 00100 19210 50603 19201 40024
00111 40320 14001 01505 03010 31301 00070 01921 07000 10019

05070 91300 07001 90905 13050 20419 00041 40311 07002 40002 07050 90001 04030 90019 04140 20005 14080 40709 07001 32104 14070 02107 00011 21105 24000 91412 140031 30506 03190 51100
On se doute qu'il y parle de villes de Ligurie comme Finale, Savone et Spotorno.
Avec ces indications, saurez-vous décrypter ce message ?

Les petits chiffres pouvaient être de simples substitutions alphabétiques, comme dans la dépêche émise par le commandant français Pulier pendant la première campagne d'Italie (voir le CQFD précédent). Mais il pouvait aussi s'agir de dictionnaires chiffrés d'une centaine de mots… avec des passages en clair. Dans les deux cas, les secrets qu'ils gardaient n'étaient pas bien durs à percer. Il ne fallut ainsi que deux jours à Scovell pour casser le petit chiffre de l'armée française du Portugal en 1811.

En principe, les grands chiffres étaient comparables aux tables de chiffrement antérieures. Cependant, pour gagner du temps, on prit la mauvaise habitude d'écrire en clair et de ne cacher que ce qu'on estimait secret. Le décryptement demande de bien connaître la situation bien sûr, mais il demeure relativement facile pour un bon linguiste. Voici un exemple qui figure dans les archives de Scovell. La ville fortifiée de Rodrigo était assiégée par les Britanniques quand le général Montbrun, commandant la division de la cavalerie française, envoya un message qui fut intercepté par les hommes de Scovell. Dans le premier paragraphe, Montbrun prend acte du précédent message de la veille, puis continue ainsi :

> Je m'empresse d'en transmettre le contenu à 25. 13. 8. 9. 38. 19. 18. 37. 14. 10. 33. 28. 17. 34. 14. 17. 26. 5. 19. 21. 23. 31. 32 qui m'a ordonné de communiquer avec vous.

Voyons le raisonnement de Scovell. Qui pouvait bien ordonner quelque chose à un général de division, sinon le général commandant l'armée lui-même, en l'occurrence le

maréchal Marmont ? La longueur même de la partie chiffrée (23 nombres !) incitait à penser que le chiffreur de Montbrun avait eu recours aux titres les plus pompeux de Marmont, comme ceux d'Excellence, de Maréchal et de Duc de Raguse. Quelques essais permettent de trouver une possibilité en 23 lettres :

S.E. Le Maréchal, Duc de Raguse

Les quelques répétitions de chiffres (14, 17 et 19) sont conformes à l'hypothèse, puisqu'ils se déchiffrent deux fois de la même façon (C, D, et A). C'est ainsi que la petite devinette facile en 23 lettres que nous venons de résoudre fournit ainsi vingt équivalents, et cinq façons de chiffrer E ! Inutile de dire qu'un petit chiffre ne pouvait résister longtemps à ce genre de bévues… Ce simple travail de Scovell lui livra près de 20 % du tableau de chiffrement. Nous retrouverons ce type d'erreurs des chiffreurs jusqu'à la Seconde Guerre mondiale, comme nous le verrons plus loin (voir le chapitre 11).

Quand, en 1813, des défections survinrent parmi les alliés de Napoléon et fournirent à leurs ennemis des tables de chiffrement, on conçoit que de nouveaux chiffres auraient été les bienvenus pour les Français. Malheureusement, la précaution de Rossignol et de Puisieulx de toujours disposer d'un chiffre de réserve avait été oubliée et l'armée napoléonienne avait en réalité… toujours un chiffre de retard sur ses ennemis. L'armée française finit par adapter le chiffre de Puisieulx de 1750, initialement prévu pour la diplomatie. Cette origine limitait les termes militaires, ce qui réduisait le nombre de codes effectifs.

Décidément, les codes secrets n'étaient pas le fort de l'armée napoléonienne : pendant la campagne de Russie aussi, en 1812, la Grande Armée communiquait à travers un petit chiffre de 240 codes pour cacher les parties qui n'étaient pas laissées en clair… Si bien que, de l'aveu même du tsar Alexandre I^{er}, les services de renseignements

russes interceptaient et décryptaient l'essentiel des dépêches de Napoléon. La paix revenue, voici ce que le tsar dit au maréchal Macdonald pour le consoler des défaites françaises :

> Nous fûmes grandement aidés parce que nous connaissions toujours les intentions de votre empereur d'après ses propres dépêches. Et nous en avons intercepté un grand nombre au cours des dernières campagnes.

Ce à quoi le maréchal répondit :

> Il n'est pas surprenant que vous ayez pu les lire, un traître vous en avait certainement livré la clef.

Le tsar rétorqua :

> Pas du tout. Je vous donne ma parole d'honneur qu'il n'en a rien été. Nous les avons simplement décryptées.

La Grande Armée = la Grande Photocopieuse

Quelles erreurs commettaient donc les chiffreurs de Napoléon ? En fait, les dépêches de la Grande Armée, comme celle de Philippe II et de bien d'autres en périodes de conflit, étaient envoyées en quelques exemplaires. L'ennemi récupérait souvent plusieurs copies du même message, ce qui aurait pu être bénin… si elles avaient toutes été chiffrées de façon identique.

La reproduction se faisait apparemment à partir de l'original non chiffré, ce qui donne, par exemple, ces deux exemplaires chiffrés différemment de la même dépêche du maréchal Berthier en septembre 1813, un mois avant la bataille de Leipzig (p. suivante).

Péterswald, ce 17 septembre 1813,
Monsieur le Maréchal,
L'empereur ordonne que vous vous portiez le plus tôt possible 167. 138. 169. 106. 171. 15. 117 avec son

Péterswald, ce 17 septembre 1813,
Monsieur le Maréchal,
L'empereur ordonne que 175. 138. 167. 164. 90. 138. 167. 152. 169. 145. 53. 166. 117. 137. 103. 157. 176. 152. 167. 134. 37. 37. 117. 174. 169. 106. 171. 15. 117. 15. 132. 6. 175. 176. 126. 48. 164. 153. 126. 32. 50. 175.

infanterie, sa cavalerie et son artillerie, en ne laissant 15. 164. 138. 169. 176. 166. 35. 138. 169. 81 que ce que Sa Majesté a désigné pour 106. 78. Son principal but sera de rester 107. 87. 176. 169. 53. 52. 167. 52. 35. 138. 6. 85. 82. 52. 106. 171. 171. 15. 117 et de chasser 117. 107. 156. 169. 145. 171. 115. 167. 68 qui manœuvrent dans 20. 176. 131. 75. Vous pouvez vous rendre en droite ligne 156. 169. 40. 35. 138. 169. 81. 167. 138. 169. 87. 53. 91.
Le Prince Vice-Connétable, Major Général,
Berthier

176. 126. 25. 68. 94. 105. 122. 171. 115. 176. 15. 164. 118. 169. 166. 35. 138. 169. 81. 136. 20. 173. 138. 53. 171. 107. 87. 82. 131. 15. 52. 134. 81. 94. 137. 90. 138. 169. 106. 51. 169. 116. 168. 115. 175. 176. 126. 137. 148. 115. 6. 119. 156. 90. 3. 176. 177. 146. 146. 52. 169. 82. 131. 169. 107. 92. 126. 52. 167. 23. 53. 35. 138. 6. 61. 167. 52. 106. 171. 39. 53. 50. 52. 6. 72. 167. 177. 169. 117. 167. 137. 22. 145. 171. 115. 167. 68. 154. 107. 94. 138. 164. 126. 115. 176. 16. 115. 167. 20. 176. 131. 67. 126. 6. 145. 175. 138. 167. 126. 115. 23. 126. 68. 23. 159. 92. 53. 93. 81. 94. 137. 22. 6. 90. 35. 138. 169. 81. 174. 169. 119. 53. 115. 15.
Le Prince Vice-Connétable, Major Général,
Berthier

À cause de cette maladresse, si les deux messages sont interceptés, l'ennemi peut commencer à les décrypter de conserve. Par exemple, la première phrase « L'empereur ordonne que vous vous portiez le plus tôt possible » appelle ensuite « sur » une ville ou un lieu. Il est vraisemblable que 167 signifie S, 138, U et 169, R. De même, « en ne laissant » appelle « à » donc 15 signifie probablement A.

En reportant dans le texte, on découvre à la fin de la dépêche :

« Vous pouvez vous rendre en droite ligne 169. R. 40. 35. UR. 81. S U R 87. 53. A. », ce qui signifie vraisemblablement : « Vous pouvez vous rendre en droite ligne par telle ville (40. 35. UR. 81.) sur telle autre (87. 53. A) ». Le nom de la première ville, allemande, finit sans doute par « burg », de sorte que 35 signifie B et 81, G.

La partie entièrement chiffrée commence alors à se dévoiler. Par exemple, le « vous vous » a été chiffré en « 175. U. S. 164. 90. U. S. » donc 175 signifie VO, 164, V et

90, O. Ces équivalences facilitent la progression, au point que l'avant-dernière ville se dévoile : il s'agit de Coburg. Une carte d'Allemagne laisse alors penser que la dernière ville, dont le nom finit par A, est Iéna. En continuant ainsi, on finit par découvrir la dépêche de Berthier :

> L'empereur ordonne que vous vous portiez le plus tôt possible sur la Saale, avec son infanterie, sa cavalerie et son artillerie, en ne laissant à Wurtzburg que ce que Sa Majesté a désigné pour la garnison. Son principal but sera de rester maître des débouchés de la Saale et de chasser les partisans ennemis qui manœuvrent dans cette direction. Vous pouvez vous rendre en droite ligne par Coburg sur Iéna.

D'un empereur à l'autre

Le chiffre de Napoléon III semble avoir été encore plus faible que celui de Napoléon I^{er}. L'armée française commença la guerre de 1870 avec un dictionnaire chiffré conçu pour la diplomatie. Dès les premières batailles, le maréchal Bazaine télégraphiait à Paris : « le chiffre destiné à la transmission des dépêches est très incommode et ne renferme aucun des termes techniques usités à la guerre ». Les mots tels que « ennemi », « bataillon », « artillerie » devaient être découpés en lettres ou syllabes, ce qui facilitait leur décryptement.

Quand Bazaine se replia dans Metz avec son armée, les Allemands encerclèrent la place forte. L'autre armée française, sous les ordres du maréchal Mac Mahon, entreprit de communiquer par télégraphe optique pour convenir d'une action coordonnée visant à dégager Bazaine et à forcer les Allemands à lever le siège. Malheureusement, ces derniers interceptaient et décryptaient sans problème les messages français, si bien qu'ils purent concentrer leurs forces au point d'attaque. La sortie de Bazaine fut repoussée et Mac Mahon vaincu. Plus tard, la victoire allemande de Sedan scella cette défaite et mit un terme à la guerre. Dans un sens, l'échec français de 1870 fut donc

aussi celui du renseignement et du chiffre… ce qui, paradoxalement, ouvrit la voie à l’excellence française durant la Grande Guerre.

6

Les chiffres par transposition

Si cet ouvrage n'était pas consacré aux codes secrets mais à l'histoire de la littérature, ce chapitre serait dédié aux anagrammes. Comme « niche » est une anagramme de « chien », « aimer » de « Marie », « baignade » de « badinage », certains codes secrets s'adonnent aux jeux de mots et s'amusent à mélanger les lettres du message transmis, afin de mieux brouiller les pistes. En cryptographie, l'anagramme devient ainsi le chiffrement par transposition. À l'instar de la substitution, cette technique est ancienne et demande, comme son équivalent littéraire, des qualités linguistiques certaines. Quand le secret des champs de bataille rejoint les jeux de lettres comme le scrabble…

La scytale

Le générateur d'anagrammes le plus simple et le plus ancien de l'Histoire qui servit à coder des messages fut la scytale. Plutarque (47-120) en parle dans sa *Vie de Lysandre*. Il y rapporte la manière utilisée par les magistrats de Sparte (les éphores) pour communiquer avec leurs généraux en campagne :

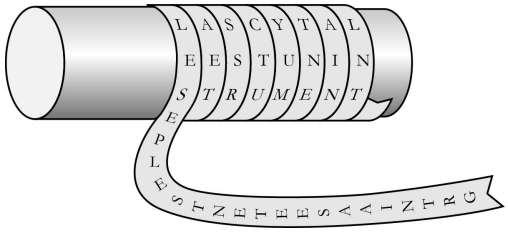
Quand un général part pour une expédition de terre ou de mer, les éphores prennent deux bâtons ronds, d'une longueur et d'une grandeur si parfaitement égales, qu'ils s'appliquent l'un à l'autre sans laisser entre eux le moindre vide. Ils gardent l'un de ces bâtons, et donnent l'autre au général ; ils appellent ces bâtons scytales. Lorsqu'ils ont quelque secret important à faire passer au général, ils prennent une bande de parchemin, longue et étroite comme une courroie, la roulent autour de la scytale qu'ils ont gardée, sans y laisser le moindre intervalle, en sorte que la surface du bâton est entièrement couverte. Ils écrivent ce qu'ils veulent sur cette bande ainsi roulée, après quoi ils la déroulent, et l'envoient au général sans le bâton.

Quand celui-ci la reçoit, il ne peut rien lire, parce que les mots, tous séparés et épars, ne forment aucune suite. Il prend donc la scytale qu'il a emportée, et roule autour la bande de parchemin, dont les différents tours, se trouvant alors réunis, remettent les mots dans l'ordre où ils ont été écrits, et présentent toute la suite de la lettre. On appelle cette lettre scytale, du nom même du bâton, comme ce qui est mesuré prend le nom de ce qui lui sert de mesure.

Le procédé est facile à mettre en œuvre : on écrit sur le papier enroulé autour de la scytale, on le déroule et le message devient alors incompréhensible, comme le montre cet exemple :

LESPN UENAE TETTT MSSRR DETEC TUMER RSYUM EPLES TNETE ESAAI NTRSD GLNTA MLUE

Pour déchiffrer le message, il faut à nouveau enrouler la lanière autour d'un bâton, comme illustré p. suivante.



On écrit sur un ruban enroulé autour d'un bâton, appelé scytale. Une fois déroulé, le message devient incompréhensible. Nous avons écrit les lettres en majuscules car les lettres cursives (avec ligatures) ne sont apparues qu'à l'époque byzantine.

Décryptement sans bâton

Imaginez maintenant que vous n'avez pas de bâton. Est-il toujours possible de décrypter le message ? Oui, en le découpant en bandes de papiers de même longueur. Accolés les unes aux autres, ces morceaux de message forment un rectangle, ou un tableau si l'on préfère. Que le rectangle ait les bonnes dimensions et il suffira ensuite de lire ce tableau colonne après colonne pour déchiffrer la missive.

Comment trouver les bonnes longueurs et largeurs du rectangle ? *A priori*, nous ne connaissons que le produit de ces dimensions : c'est la longueur du message sur le ruban :
LESPNUENAETETTTMSSRRDETECTUMERRSYUMEPLESTNETEESAAINTRSDGLNTAMLUE

Elle est ici de 64 lettres. Plusieurs produits de dimensions sont possibles, mais les plus vraisemblables sont 8 fois 8 et 16 fois 4. Les décompositions en 4 longueurs de 16 et en 8 longueurs de 8 donnent :

LESPNUENAETETTTM	LESPNUEN
SSRRDETECTUMERRS	AETETTTM
YUMEPLESTNETEESA	SSRRDETE
AINTRSDGLNTAMLUE	CTUMERRS
	YUMEPLES
	TNETEESA
	AINTRSDG
	LNTAMLUE

Lu en colonne, seul le second texte a un sens : « la scytale est un instrument permettant de permuter les lettres d'un message ». Le déchiffrement est quand même plus simple avec un bâton, n'est-ce pas ?

Ce Qu'il Faut Décrypter

La scytale

Le message suivant a été chiffré au moyen d'une scytale :

CAECI NDREE AYRCE NMTVT CELEE EEAOH OUSCC LNUNF SRUEF IGRAY NDETU VGPEE REELE TSCET U

Saurez-vous le décrypter ?

Le chiffre *rail fence* ou zigzag

Un chiffre par transposition simple, qui a été employé durant la guerre de Sécession par les deux camps, mais dont on ignore l'origine exacte, consiste à écrire le message à chiffrer sur plusieurs lignes en alternant, par exemple dispersé sur deux lignes : c'est le zigzag, ou *rail fence* (« palissade », en référence aux clôtures dessinant ce motif). Ainsi, la phrase « un message se crée » s'écrit d'abord :

U M S A E E R E

N E S G S C E

La version chiffrée se lit ensuite ligne après ligne :

UMSAE ERENE SGSCE

Réparti sur trois lignes, le message devient :

U S E R

N E S G S C E

M A E E

USERN ESGSC EMAEE

On continue ainsi sur autant de lignes qu'on veut, à condition toutefois que le message soit suffisamment long. Dès que l'on connaît la méthode et le nombre de lignes utilisées, le déchiffrement est facile. Dès lors que les fréquences sont normales, le chiffrement ne comporte pas de substitution, de sorte qu'un chiffre par transposition est

envisageable, ce qui conduit à essayer le *rail fence* avec deux lignes, trois lignes, etc. On peut varier la méthode en commençant le zigzag de façon différente.

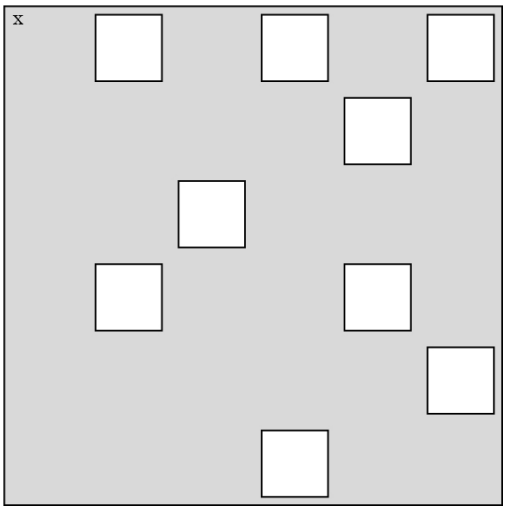
Ce Qu'il Faut Décrypter

Le *rail fence*

Le message suivant a été chiffré au moyen d'un *rail fence* :
CSEEF PNLCR IGEES GATCI FEAUR IFNEU TOSIN SMAEH RRAES RLE
Saurez-vous le décrypter ?

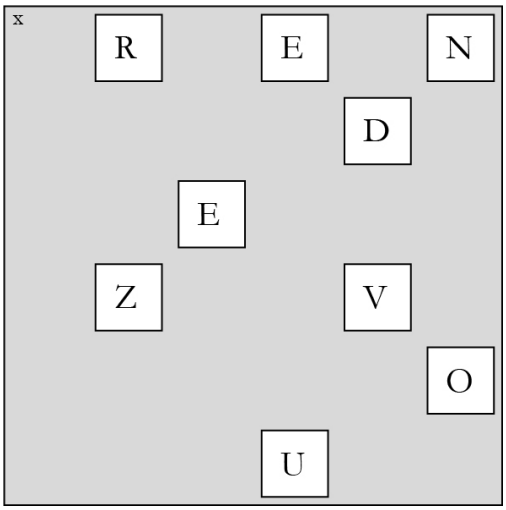
Les grilles tournantes

Dans l'Histoire, il y a eu les tables tournantes qui permettaient aux esprits d'envoyer des messages aux simples mortels que nous sommes et les… grilles tournantes grâce auxquelles on communiqua de façon secrète au XIX^{e} siècle. Dans son livre sur la cryptographie (*Handbuch der Kryptographie*), le colonel autrichien Edouard Fleissner von Wostrowitz (1825-1888) décrit ce système qui fournit des transpositions de textes, composées de 36 lettres dans l'exemple. Il fonctionne à partir d'un carré en carton de 6 cm sur 6 cm, sur lequel sont dessinés 36 petits carrés de 1 cm de côtés (non visibles sur le dessin). 9 de ces petits carrés sont ajourés.



Une grille tournante de côté six.

La petite croix figurant en haut et à gauche de la grille est nécessaire pour repérer sa position initiale. Les cases ajourées ont été choisies de telle façon que, si on tourne trois fois la grille de 90° dans le sens des aiguilles d'une montre, elles recouvrent le carré entier. Pour montrer comment chiffrer avec cette grille tournante, chiffrons le message : « rendez-vous à midi au palais du Trocadéro ». À la première étape, on chiffre les 9 premières lettres « RENDEZVOU » en posant la grille sur le papier et en remplissant les trous dans l'ordre (voir la première étape du chiffrement sur la figure ci-contre).



Première étape du chiffrement.

On recommence avec la suite du message, en tournant trois fois la grille de 90° dans le sens des aiguilles d'une montre. Comme le texte ne fait que 34 lettres, il faut le compléter avec deux X (voir le chiffrement final ci-contre).

O	R	A	E	C	N
L	A	S	D	D	A
E	A	E	M	I	R
I	Z	O	S	V	D
X	D	I	X	A	O
U	U	T	U	R	P

Le chiffrement final.

Nous pouvons l'écrire en ligne : « ORAEC NLASD DAEAE MIRIZ OSVDX DIXAO UUTUR P » et l'envoyer ainsi. Pour

déchiffrer, il suffit de reprendre les mêmes opérations à l'envers.

Le chiffre de Jules Verne

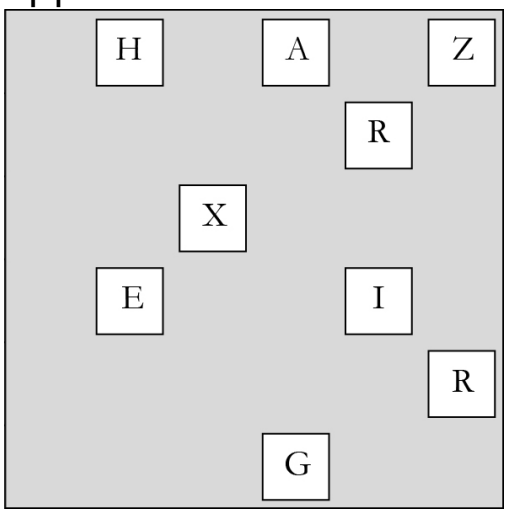
Un message chiffré par grille tournante est au cœur du roman de Jules Verne paru en 1885, *Mathias Sandorf*. Le voici tel qu'il apparaît dans le livre :

IHNALZ	ZAEMEN	RUIOPN
ARNURO	TRVREE	MTQSSL
ODXHNP	ESTLEV	EEUART
AEEEIL	ENNIOS	NOUPVG
SPESDR	ERSSUR	OUITSE
EEDGNC	TOEEDT	ARTUEE

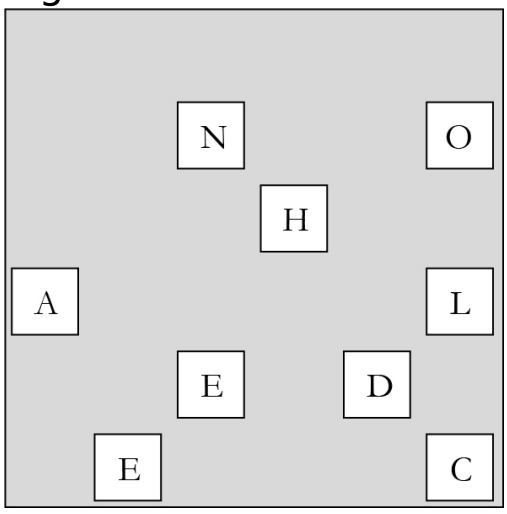
Ayant découvert une grille tournante (aux mêmes dimensions et découpée de façon identique à celle décrite plus haut), les héros l'appliquent sur chaque colonne de la liste. Les mots de chaque colonne forment en effet un carré de 36 lettres. Le premier est :

I	H	N	A	L	Z
A	R	N	U	R	O
O	D	X	H	N	P
A	E	E	E	I	L
S	P	E	S	D	R
E	E	D	G	N	C

En plaçant la grille ajourée sur ce carré, seules 9 lettres apparaissent :



On fait alors tourner la grille de 90° dans le sens des aiguilles d'une montre :



En recommençant deux fois, le premier carré donne le (peu) clair :

HAZRXEIRG NOHALEDEC NADNEPEDN ILRUOPESS

Malgré le manque de sens apparent, les héros ne se découragent pas, recommencent sur les deux autres carrés et obtiennent :

AMNETNORE VELESSUOT ETSEIRTED ZERREVNES
UONSUOVEU QLANGISRE IMERPUATE RPTSETUOT

Cela semble encore plus obscur quand l'un d'eux pense à lire à l'envers le message, qui s'éclaire alors : « Tout est prêt. Au premier signal que vous nous enverrez de Trieste,

tous se lèveront en masse pour l'indépendance de la Hongrie. Xrzah ».

Le texte avait été surchiffré en l'écrivant à l'envers, la plus simple transposition qui soit ! L'armée allemande utilisa ce chiffre pendant la Première Guerre mondiale pour des communications de proximité. Comme tous les autres, il fut cassé par l'armée française.

Ce Qu'il Faut Décrypter

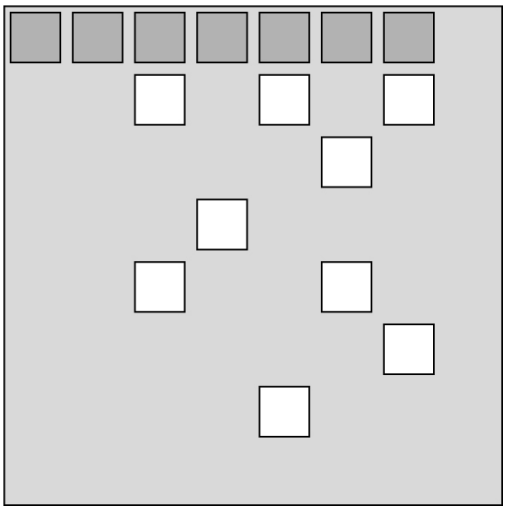
La grille tournante

Le message suivant a été chiffré au moyen d'une grille tournante de côté six :

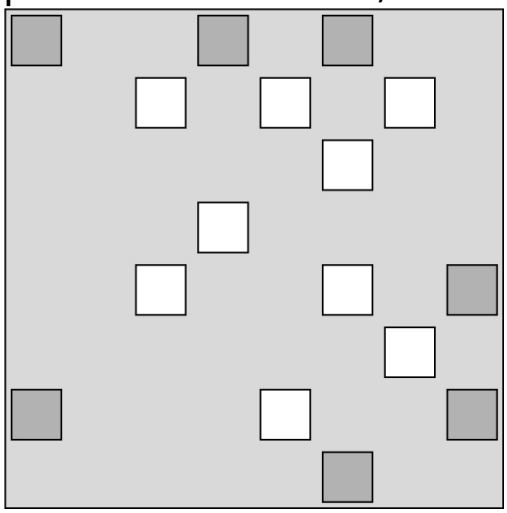
NLRAEL NMEALV GEEARI CMNLAO OANTTG LOINGU

Saurez-vous le décrypter ?

Bien entendu, on peut fabriquer des grilles tournantes de tout côté pair. N'essayez pas d'en fabriquer de côté impair, c'est impossible. Pourquoi ? Tout simplement parce que le carré d'un nombre impair n'est pas divisible par 4 ! Commençons donc par concevoir un carré de côté huit : on part de celui de côté six et on le borde par des rangées de carrés de côté un. La solution la plus simple serait de remplir d'abord les sept premiers carrés de la ligne supérieure.



La grille obtenue convient du point de vue géométrique, puisqu'on remplit le carré en la faisant tourner trois fois de 90° dans le sens des aiguilles d'une montre. En revanche, elle ne convient pas du point de vue cryptographique, puisque certaines parties du message resteraient en clair. Pour y remédier, il suffit de remarquer que chaque case grisée peut être remplacée par une de celles qu'on obtient en faisant tourner la grille de 90°, 180° ou 270°. Cela fournit plusieurs solutions, dont celle-ci :



Les grilles tournantes sont une façon simple, rapide et plutôt efficace de chiffrer un message. MAIS elles exigent de transmettre et de garder précautionneusement un secret, en l'occurrence la grille. De ce point de vue, elles

contreviennent au principe de Kerckhoffs. Niveau sécurité, elles sont bonnes à jeter à la poubelle.

Ce Qu'il Faut Décrypter

La grille tournante de côté huit

Le message suivant a été chiffré au moyen d'une grille tournante de côté huit :
DQAEAMRU TLATREAA SQTEHTLE UREEERMS OPPPLREE RYASLEVS IGVREEON ENCTETSP
Quel est le message en clair ?

Le chiffre du *Voyage au centre de la Terre*

Restons avec Jules Verne, grand amateur de jeux de l'esprit. Dans le *Voyage au centre de la Terre*, une partie de l'intrigue repose sur un autre chiffre à transposition. Les héros découvrent un parchemin avec une inscription en runes, des caractères islandais :

Après l'avoir traduit en caractères latins, ils trouvent le texte suivant :

mm.rnlls	esreuel	seecJede
sgtssmf	unteief	niedrke
kt,samn	atrateS	Saodrrn
emtnael	nuaect	rrilSa
Atvaar	nscrc	ieaabs

ccdrmi	eeutul	frantu
dt,iac	oseibo	KediiY

Les héros ont alors l'idée de lire les premières lettres de chaque groupe dans l'ordre habituel de la lecture :

mmessunkaSenrA.icefdoK.segnittamurtnecertse rrette,rotaivsadua,ed necsedsadnelacartniiil uJsiratracSarbmutabil edmekmeretarcsilucoYs leffenSnl

Cette opération réalise une transposition du texte original. *A priori*, ce texte n'a aucun sens, sauf si, comme dans *Mathias Sandorf*, on lit ce texte à l'envers pour trouver un texte en latin du Moyen Âge :

In Sneffels Yoculi craterem kem delibat umbra Scartaris Julii intra calendas descende, audas viator, et terrestre centrum attinges. Kod feci. Arne Saknussemm.

En français, cela donne :

Descends dans le cratère du Yocul de Sneffels que l'ombre du Scartaris vient caresser avant les calendes de Juillet, voyageur audacieux, et tu parviendras au centre de la Terre. Ce que j'ai fait.
Arne Saknussemm.

Que l'aventure commence !

Ce Qu'il Faut Décrypter

Un message du centre de la Terre

Le message suivant a été chiffré au moyen du chiffre du *Voyage au centre de la Terre* :

ramesv	greomsa	negceur
itaécéB	nayrrr	hlofez
eevfte	Ldeipv	éelhya
vrscrs	rtnecu	enagéo
Hedadv	cesà,	eumsio

Saurez-vous y voir clair ?

Transpositions rectangulaires

Revenons au chiffrement par scytale, qui a le mérite de dépendre d'une clef : le diamètre du bâton qui, bien entendu, n'est pas divulgué, ce qui répond au principe de Kerckhoffs. Je vais vous montrer qu'avec un brin d'esprit mathématique, il est possible de généraliser son principe. Comme nous l'avions remarqué, son fonctionnement peut être simulé à l'aide d'un rectangle. Écrivons notre premier message en lignes dans un carré de côté 8.

L	A	S	C	Y	T	A	L
E	E	S	T	U	N	I	N
S	T	R	U	M	E	N	T
P	E	R	M	E	T	T	A
N	T	D	E	P	E	R	M
U	T	E	R	L	E	S	L
E	T	T	R	E	S	D	U
N	M	E	S	S	A	G	E

L'utilisation d'une scytale revient à écrire un message en ligne dans un rectangle, puis à le transmettre en colonne.

Chiffrer avec une scytale revient à extraire les colonnes de ce tableau. Mathématiquement, cela équivaut à effectuer une certaine permutation. Mais d'autres transformations sont envisageables. La difficulté est alors de retenir la transposition mobilisée, sans la noter si possible, pour répondre au principe de Kerckhoffs : vos notes doivent pouvoir tomber aux mains de l'ennemi sans affaiblir la

méthode de chiffrement. Le principe doit donc être fondé sur une idée simple.

Plusieurs méthodes sont possibles : combinatoires ou géométriques. La première idée est d'échanger les colonnes du rectangle. Pour cela, il suffit de se donner une permutation des nombres de 1 à 8, si le rectangle a 8 colonnes comme dans notre exemple. Permuter les colonnes revient à les numéroter dans le désordre : ainsi, « 78513642 » peut signifier que l'on doit recopier la colonne notée 1 en septième position, puis la 2 en huitième, etc.

7	8	5	1	3	6	4	2
L	A	S	C	Y	T	A	L
E	E	S	T	U	N	I	N
S	T	R	U	M	E	N	T
P	E	R	M	E	T	T	A
N	T	D	E	P	E	R	M
U	T	E	R	L	E	S	L
E	T	T	R	E	S	D	U
N	M	E	S	S	A	G	E

1	2	3	4	5	6	7	8
C	L	Y	A	S	T	L	A
T	N	U	I	S	N	E	E
U	T	M	N	R	E	S	T
M	A	E	T	R	T	P	E
E	M	P	R	D	E	N	T
R	L	L	S	E	E	U	T
R	U	E	D	T	S	E	T
S	E	S	G	E	A	N	M

Permutation des colonnes : la colonne notée 7 du premier rectangle va en septième position dans le second, et ainsi de suite.

Cependant, sauf pour un amoureux des nombres, il est difficile de mémoriser une suite de chiffres comme « 78513642 ». Il est plus simple de se souvenir d'un mot ayant un sens, comme « RVLEHNING ». Comment passer de l'un à l'autre ? Rien de plus simple. On classe d'abord les lettres de « RVLEHNING » dans l'ordre alphabétique : « EGHILNRV ». Dans « RVLEHNING », chaque lettre est alors remplacée par son ordre d'apparition dans « EGHILNRV », si l'on exclut les doublons. Ainsi, la clef « RVLEHNING » cache la permutation « 78513642 ». Elle donne la transposition suivante du message initial :

CTUME RRSLN TAMLU EYUME PLESA INTRS DGSSR RDETE TNETT TSALE SPNUE NAETE TTTM.

Décryptement sans la clef

La section précédente va nous aider à développer une méthode générale de décryptement. Si jamais les fréquences d'un message chiffré sont celles que l'on trouve dans un texte normal, comme nous l'avons déjà dit, il est probable qu'il ait été chiffré par transpositions. Vu les paragraphes précédents, votre réflexe devrait être, face à un tel message, de l'écrire sous forme de lignes dans un tableau rectangulaire, puis d'essayer des permutations de colonnes pour le décrypter. Prenons le message codé :

EOSER EETUN OXTIU LQNPU AEANA SEERI ETAIN TADDI CERTG PTUET DNPSA SCIOT EUEOT EIUCS GCNRI DCXSO DTROL UUTAT LDDPC ELLEB

Les fréquences des lettres sont usuelles. Nous avons donc affaire à un chiffrement par transposition. La longueur du message est égale à 100. Le tableau rectangulaire peut être 10 fois 10, 20 fois 5, 25 fois 4, etc. Si nous essayons 10 fois 10, nous sommes amenés à considérer les colonnes suivantes.

Nous cherchons alors des arrangements conférant un sens à la première ligne. Bien entendu, l'existence de mots probables simplifie cette tâche *a priori* fastidieuse. La recherche d'anagrammes n'est jamais un travail facile ! Dans la première ligne, « EOAECDEGDL », nous trouvons quatre mots possibles : « code », « décode », « codage » et « décodage ». En effectuant les permutations correspondantes, nous ne retenons que celle qui donne un résultat pour les autres lignes. Voici donc la première étape :

E	O	A	E	C	D	E	G	D	L
O	X	E	T	E	N	U	C	T	D
S	T	A	A	R	P	E	N	R	D
E	I	N	I	T	S	O	R	O	P
R	U	A	N	G	A	T	I	L	C
E	L	S	T	P	S	E	D	U	E
E	Q	E	A	T	C	I	C	U	L
T	N	E	D	U	I	U	X	T	L
U	P	R	D	E	O	C	X	A	E
N	U	I	I	T	T	S	O	T	B

Disposition du message en colonnes. Il reste maintenant à les ordonner.

D	E	C	O	D	A	G	E	E	L
N	T	E	X	T	E	C	O	U	D
P	A	R	T	R	A	N	S	E	D
S	I	T	I	O	N	R	E	O	P
A	N	G	U	L	A	I	R	T	C
S	T	P	L	U	S	D	E	E	E
C	A	T	Q	U	E	C	E	I	L
I	D	U	N	T	E	X	T	U	L
O	D	E	P	A	R	X	U	C	E
T	I	T	U	T	I	O	N	S	B

Première étape du décryptement.

Après cette étape, il reste « EL » dans la première ligne, qui donne « LE » à placer en tête, d'où la dernière étape.

L	E	D	E	C	O	D	A	G	E
D	U	N	T	E	X	T	E	C	O
D	E	P	A	R	T	R	A	N	S
P	O	S	I	T	I	O	N	R	E
C	T	A	N	G	U	L	A	I	R
E	E	S	T	P	L	U	S	D	E
L	I	C	A	T	Q	U	E	C	E
L	U	I	D	U	N	T	E	X	T
E	C	O	D	E	P	A	R	X	U
B	S	T	I	T	U	T	I	O	N

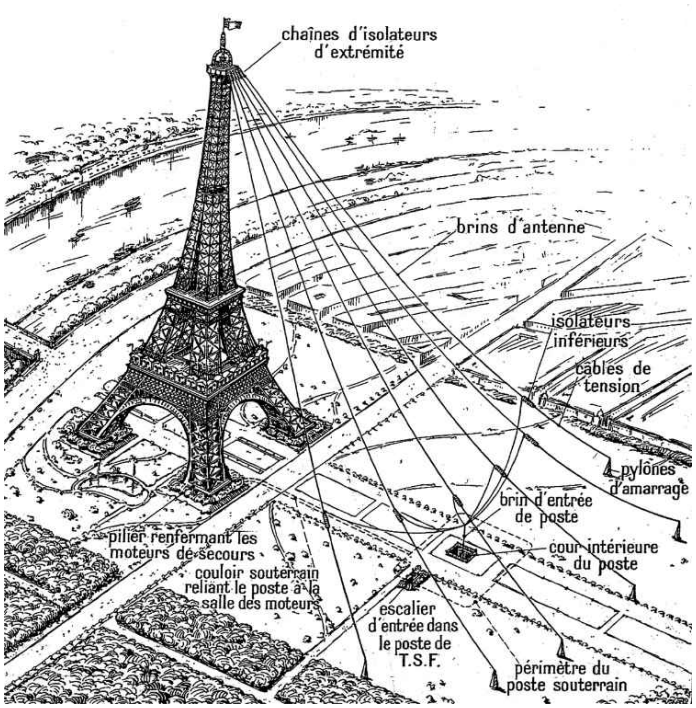
Dernière étape.

Il reste à lire le texte en lignes : « le décodage d'un texte codé par transposition rectangulaire est plus délicat que celui d'un texte codé par substitution ». Cette phrase ayant un sens, nous avons visiblement réussi à décrypter le message. L'affirmation contenue dans celui-ci dépend en fait de chaque cas particulier. Ici le décryptement était particulièrement facile. En général, dans la recherche d'anagramme, la méthode du mot probable constituera toujours une aide. Il est plus facile de trouver ce que l'on cherche que de partir complètement au hasard !

Le système Übchi

Au début de la Première Guerre mondiale, à la différence de la diplomatie et de la marine qui préféraient utiliser des livres de codes, l'armée allemande recourait à un chiffre à base d'une transposition de lignes et non de colonnes. Il était nommé Übchi, un acronyme signifiant curieusement *Übungen der Chiffre* (« exercices de chiffre »). Arrêtons-nous un instant sur ce choix d'un chiffre plutôt que d'un code, car il répond au principe de Kerckhoffs. Un code s'appuie sur le

secret total, un chiffre est censé reposer sur une clef, que l'on change périodiquement et que l'on ne note pas, afin d'éviter qu'elle tombe entre les mains de l'ennemi.


chaînes d'isolateurs d'extrémité
brins d'antenne
isolateurs inférieurs
cables de tension
pylônes d'amarrage
brin d'entrée de poste
cour intérieure du poste
pilier renfermant les moteurs de secours
couloir souterrain reliant le poste à la salle des moteurs
escalier d'entrée dans le poste de T.S.F.
périmètre du poste souterrain

La tour Eiffel et ses antennes en 1914. De nos jours, l'entrée du poste de TSF est encore visible.

Les principes du chiffre Übchi étaient connus de l'armée française, avant même la guerre (l'armée disposait elle-même d'un chiffre du même type). *A priori*, cette connaissance n'était pas un problème en soi pour les Allemands, car le chiffre exigeait l'emploi d'une clef qui était changée périodiquement, tous les huit jours environ. Ce qu'ils ignoraient en revanche, c'est que les décrypteurs français avaient mis au point une méthode pour découvrir la clef ! Inspirée de celle que nous avons décrite, elle ne réclamait que quelques messages de longueur égale pour fournir la clef.

Pas de chance pour les Allemands : pendant la guerre de mouvement de 1914, la « grande oreille » de la tour Eiffel interceptait des milliers de messages par jour. Parmi ceux-ci fut saisi un ordre d'attaque du général Karl von Richthofen, daté du 31 août et chiffré avec un Übchi. La missive confirmait le changement de direction de la progression allemande, qui avait été remarqué également par l'aviation. L'armée allemande offrait son flanc droit au lieu de contourner l'armée française. Grâce au message, le général Joffre lança une contre-offensive qui dissocia l'aile droite allemande et la força à la retraite. Cet épisode porte aujourd'hui le nom de bataille de la Marne.

Les détails d'Übchi

Comment fonctionnait le système allemand ? Il nécessitait une clef, qui était un mot ou une phrase, comme « domination ». Il s'agit en fait d'un moyen mnémotechnique, qui permet de retenir une suite de chiffres, ici 10. Notre exemple est en français pour faciliter la compréhension, mais les principes restent les mêmes en allemand.

D	O	M	I	N	A	T		I	O	N
2	**8**	**5**	**3**	**6**	**1**	**10**		**4**	**9**	**7**

Création d'une suite de chiffres à partir de la clef : on numérote simplement les cases dans l'ordre alphabétique. La première ici est A, la suivante D, etc.

Le message « ordre à la première armée, attaquer demain vers Vauxaillon » se chiffre alors en formant un tableau de dix colonnes, qu'on complète par des nulles si besoin, ici Z.

2	**8**	**5**	**3**	**6**	**1**	**10**	**4**	**9**	**7**
O	R	D	R	E	A	L	A	P	R
E	M	I	E	R	E	A	R	M	E
E	A	T	T	A	Q	U	E	R	D
E	M	A	I	N	V	E	R	S	V
A	U	X	A	I	L	L	O	N	Z

Première étape du chiffrement.

Nous en déduisons un nouveau texte en prenant les colonnes dans l'ordre indiqué par la clef :

AEQVL OEEEA RETIA ARERO DITAX ERANI REDVZ RMAMU PMRSN LAUEL

Ce nouveau texte est recopié en lignes dans le tableau.

2	**8**	**5**	**3**	**6**	**1**	**10**	**4**	**9**	**7**
A	E	Q	V	L	O	E	E	E	A
R	E	T	I	A	A	R	E	R	O
D	I	T	A	X	E	R	A	N	I
R	E	D	V	Z	R	M	A	M	U
P	M	R	S	N	L	A	U	E	L

Seconde étape du chiffrement.

On reprend ensuite la première étape, en recopiant les colonnes dans l'ordre donné par la clef :

OAERL ARDRP VIAVS EEAAU QTTDR LAXZN AOIUL EEIEM ERNME ERRMA

Chiffrés de cette manière, les messages allemands étaient transmis par radio… et immédiatement captés par les antennes de la tour Eiffel. Comme nous l'avons vu, le travail

des décrypteurs français était certes laborieux, mais quelques messages de même longueur avec la même clef suffisaient pour reconstituer le texte originel. Leur tâche fut même parfois facilitée par les chiffreurs allemands, qui oubliaient la deuxième permutation. Dans ce cas, la reconstitution de la clef était une question d'heures au lieu de jours.

L'incroyable bévue du *Matin*

Dans le monde des cryptologues, excepté le chevalier de Rohan qui en perdit la tête, il n'est pas dans les habitudes de se vanter de ses exploits. On comprend aisément pourquoi ! L'inverse est même plutôt de rigueur (« Nous, décrypter les messages ennemis ? Nous ne sommes pas assez intelligents pour y parvenir. ») Pourtant, c'est un journal français, *Le Matin*, qui fit comprendre aux Allemands que les Français lisaient par-dessus leurs épaules.

En octobre 1914, l'armée française intercepta un message chiffré annonçant que l'empereur Guillaume II visiterait la ville belge de Thielt. Les avions français furent au rendez-vous (même s'ils ratèrent l'empereur)… et *Le Matin* fut très fier d'annoncer ce succès français du renseignement militaire. Le résultat ne se fit pas attendre : un mois plus tard, les Allemands changeaient leur chiffre.

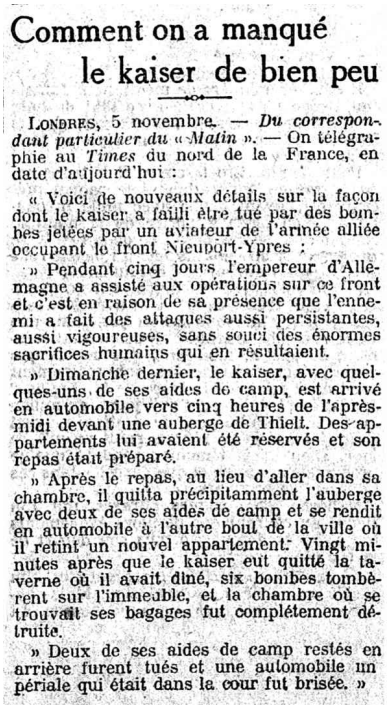
Cette bévue rappelle celle du *Temps* qui, en 1870, annonça la manœuvre du maréchal Mac Mahon pour secourir le maréchal Bazaine encerclé dans Metz… avec les conséquences désastreuses que l'on connaît.

Un message en Übchi

Le message suivant a été chiffré au moyen du chiffre Übchi :

FDTON EFNXM IXSER UORAE DELGE ARNSA TERUR TIERA RERHV OCIN

Que signifie-t-il, sachant que notre espion a découvert que la clef de chiffrement était « loyauté » ?



Comment on a manqué le kaiser de bien peu

LONDRES, 5 novembre. — *Du correspondant particulier du « Matin »*. — On télégraphie au *Times* du nord de la France, en date d'aujourd'hui :

« Voici de nouveaux détails sur la façon dont le kaiser a failli être tué par des bombes jetées par un aviateur de l'armée alliée occupant le front Nieuport-Ypres :

» Pendant cinq jours l'empereur d'Allemagne a assisté aux opérations sur ce front et c'est en raison de sa présence que l'ennemi a fait des attaques aussi persistantes, aussi vigoureuses, sans souci des énormes sacrifices humains qui en résultaient.

» Dimanche dernier, le kaiser, avec quelques-uns de ses aides de camp, est arrivé en automobile vers cinq heures de l'après-midi devant une auberge de Thielt. Des appartements lui avaient été réservés et son repas était préparé.

» Après le repas, au lieu d'aller dans sa chambre, il quitta précipitamment l'auberge avec deux de ses aides de camp et se rendit en automobile à l'autre bout de la ville où il retint un nouvel appartement. Vingt minutes après que le kaiser eut quitté la taverne où il avait dîné, six bombes tombèrent sur l'immeuble, et la chambre où se trouvait ses bagages fut complétement détruite.

» Deux de ses aides de camp restés en arrière furent tués et une automobile impériale qui était dans la cour fut brisée. »

Le Matin du 5 novembre 1914. Dans l'édition parue deux jours plus tôt, l'article mentionnait des « renseignements venus de Belgique », mais il était facile pour les Allemands de trouver l'origine de la fuite…

Règles inhabituelles

Les transpositions des lettres d'un message peuvent être définies de façons plus exotiques, mais il faut alors un ordinateur pour les mettre en œuvre. Voici quelques méthodes intéressantes et, à mon avis, inédites. La première part d'un carré identique à celui de Polybe associé

à une clef d'au moins 25 lettres. Nous pouvons reprendre le poème de Verlaine utilisé au chapitre précédent, en changeant toutefois la règle. Nous en déduisons une numérotation des 25 cases.

L	E	S	S	A
N	G	L	O	T
S	L	O	N	G
S	D	E	S	V
I	O	L	O	N

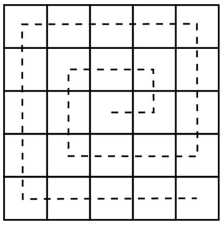
8	3	19	20	1
12	5	9	15	24
21	10	16	13	6
22	2	4	23	25
7	17	11	18	14

La clef est écrite dans le carré, ce qui permet de numéroter chaque case selon l'ordre alphabétique (1 pour A, 2 pour D car B et C sont absents, etc.).

Le message est alors écrit dans une suite de carrés de ce type. La lettre de la case numérotée 1 est mise en tête, celle de la case numérotée 2 en deuxième, etc. Nous obtenons ainsi une anagramme de chaque groupe de 25 lettres du message. Le message « voici un chiffre compliqué, eh ? » devient « CILIV FIHCE QIORU UOCEH NMFPE » (p. suivante en haut). Pour déchiffrer, il suffit d'écrire le message dans la grille, puis de lire les lettres dans l'ordre donné par la clef. On peut également fournir la règle de transposition sous diverses formes géométriques. Par exemple, en partant du centre et en poursuivant en spirale dans le sens contraire des aiguilles d'une montre.

C	I	L	I	V
F	I	H	C	E
Q	I	O	R	U
U	O	C	E	H
N	M	F	P	E

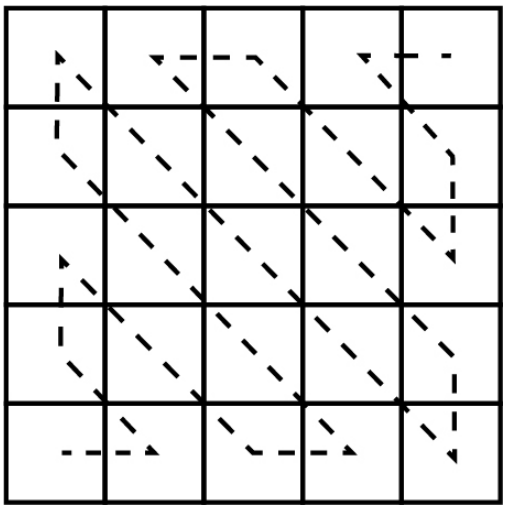
Arrangement du message selon la grille de permutation.



17	16	15	14	13
18	5	4	3	12
19	6	1	2	11
20	7	8	9	10
21	22	23	24	25

Écriture en spirale. Ce chiffre est trop régulier pour tromper, si on pense à écrire le message dans un carré.

Les idées de disposition de ce genre ne manquent pas. Une option est par exemple de tracer des diagonales en partant d'un côté ou d'un autre, etc.



Parcours en diagonales. On note 1 la case du bas, à gauche et on numérote les suivantes dans l'ordre.

Transpositions des mots

Pendant la guerre de Sécession, première guerre où les transmissions furent télégraphiques, les nordistes exploitèrent un chiffre original créé par Anson Stager (1825-1885), un cadre de la Western Union. Ce chiffre comprenait un code et une transposition. Pour éviter que les termes militaires ne soient reconnus, on transformait au préalable les mots comme « colonel », « général », « hommes », « canons », « fusils », « prisonniers », « guerre » en des termes de la langue courante comme « poupée », « odeur », « bébés », « caractères », « jouets », « jeu ». En outre, les noms propres étaient déguisés : « le président » pouvait être « Adam » et « Grant », « Noël », etc.

Comment le message était-il chiffré ? Il était écrit dans un rectangle, puis mélangé avec la règle que nous allons voir. Optons pour le texte : « Pour le colonel Nelson, nous cherchons deux correspondants de guerre. Ils ont été signalés prisonniers dans votre secteur. Pouvez-vous les trouver. Le président ». Traduisons d'abord les mots du répertoire et disposons-les dans un rectangle.

Pour	le	poupée	nelson	nous
cherchons	deux	correspondants	de	jeu
ils	ont	été	signalés	Jouets
dans	votre	secteur	pouvez	Vous
les	trouver	adam	pour	Remplir

Première étape du chiffrement.

Recopions ensuite les mots par colonnes en commençant par la première et en remontant, puis en continuant par la deuxième en haut, en descendant, etc. Ajoutons des nuls à chaque fin de colonne et un mot en en-tête indiquant le nombre de colonnes. Comme il y en a ici cinq, choisissons un mot de cinq lettres, par exemple « effet ». Voilà le résultat :

> Effet les dans ils cherchons pour baiser le deux ont votre trouver tourner adam secteur été correspondants poupée temps nelson de signalés pouvez pour ventre remplir vous jouets jeu nous

L'un des avantages de la méthode est de n'utiliser que des mots usuels, ce qui limite les risques d'erreur des télégraphistes. Pour déchiffrer, on utilise le premier mot « effet » qui donne le nombre de colonnes du tableau puis le nombre total de mots pour déterminer la longueur des colonnes. Il reste alors à le remplir en supprimant les nuls. Les sudistes semblent ne jamais avoir été capables de décrypter les messages ainsi chiffrés.

En définitive, les chiffrements par transposition ne sont pas cassables par des calculs statistiques comme les chiffrements par substitution. Ils ne deviennent solides que lorsque le message a une certaine longueur, sinon un bon linguiste retrouvera facilement le sens caché. Par exemple, trouverez-vous le sens du court message qui suit ? « Ovarb suov zeva évuort ».

7 Cryptologue… jusqu'à la folie

Vous vous souvenez du héros du film *Un homme d'exception*, sorti en 2001 ? Devenu schizophrène, il voyait des codes secrets dissimulés partout dans les articles des journaux. Il pensait que les services secrets communiquaient avec lui par cet intermédiaire. Le film racontait la vie réelle du prix Nobel d'économie et grand mathématicien John Nash, que son intelligence exceptionnelle n'avait pas immunisé contre les troubles mentaux… Pourtant, imaginer à tort qu'un nombre, un journal ou un livre comportent des messages codés était loin d'être une nouveauté. Au fil de l'Histoire, des esprits illuminés se sont crus investis du rôle de révéler par ce biais des messages de nature souvent divine. Quand l'obsession pour la cryptographie devient pathologique…

Le chiffre de la bête

À tout seigneur tout honneur. Le nombre star de l'ésotérisme, à qui on a prêté énormément de significations, est naturellement 666, le chiffre de la bête. Sa première apparition « officielle » se trouve dans l'Apocalypse de Jean, à la fin du chapitre 13 :

> C'est le moment d'avoir du discernement : celui qui a de l'intelligence, qu'il interprète le chiffre de la bête, c'est un chiffre d'homme : et son chiffre est six

cent soixante-six.

Peut-être l'évangéliste voulait-il coder un message trop dangereux ? Certains pensent ainsi que Jean se référait à travers ce chiffre à l'empereur Néron. En effet, par une manipulation sinueuse il y a moyen de transformer 666 en Néron : en ajoutant à Néron son titre, César, et en écrivant le tout en hébreu (קסר נרון), puis en ajoutant les valeurs numériques des lettres, on obtient 666. Les valeurs numériques en question sont celles qu'utilisaient les anciens Hébreux : de 1 à 10 pour les dix premières lettres (aleph א beth ב ghimel ג daleth ד he ה vav ו zayin ז het ח tet ט yod י), de 20 à 90 pour les huit suivantes (kaf כ lamed ל mem מ nun נ ou ן samech ס ayin ע pe פ tsade צ) et de 100 à 400 pour les dernières (qof ק resh ר shin ש tav ת). La valeur de ces dernières explique le score atteint par César Néron en hébreu ! Dans l'ordre, de gauche à droite, le calcul est :

50 + 6 + 200 + 50 + 200 + 60 + 100 = 666.

Il est possible que Jean ait pensé effectivement à Néron. Il est plus douteux qu'il ait songé à d'autres « bêtes ». Après lui, un certain nombre de mathématiciens se sont essayés à leur tour à la gématrie, cet art issu de la Bible hébraïque qui consiste à attribuer des nombres aux mots et aux phrases. Ces « savants » ont cherché des personnages célèbres dans le nombre 666. Par exemple, au temps des guerres de Religion, le moine et mathématicien allemand Michael Stifel (1486-1567) (qui inventa les logarithmes indépendamment de l'Écossais John Napier) montra que 666 désignait en réalité le pape de l'époque, Léon X.

Comment avait-il raisonné ? Pour le savoir, écrivez tout d'abord le nom du pape sous la forme « LEO DECIMVS », mais ne retenez que les lettres ayant un sens dans le système numérique des Romains, c'est-à-dire « LDCIMV ». Maintenant, ajoutez X puisque « LEO DECIMVS » a dix lettres et enlevez le M car c'est l'initiale du mot « mystère ». Vous obtenez « LDCIXV ». Réarrangez tout cela et vous

obtenez « DCLXVI », c'est-à-dire 666 ! Élémentaire, n'est-ce pas ?

John Napier (1550-1617) lui-même ne fut pas en reste et, à l'aide d'une autre méthode, confirma que 666 pointait bien vers Léon X. Réponse du berger à la bergère, un père jésuite opta de son côté pour Martin Luther… Son raisonnement étant plus proche du classicisme gématrique, nous l'exposons en détail. Pour lui, les lettres A à I représentaient les nombres 1 à 9, les lettres de K à S les nombres 10 à 90 (de dix en dix) et les lettres de T à Z les nombres de 100 à 500 (de cent en cent). Le nom « MARTIN LUTERA » correspond alors à l'addition :

30 + 1 + 80 + 100 + 9 + 40 + 20 + 200 + 100 + 5 + 80 + 1.

La somme vaut naturellement 666. Rendons à ce brave père jésuite l'hommage qu'il mérite. Personnellement, je n'aurais jamais pensé à une façon si tordue d'arriver au résultat ! Durant la Première Guerre mondiale, il fut démontré avec la même rigueur scientifique que 666 représentait Guillaume II, l'empereur allemand qui avait jeté son pays dans le conflit. Qui le nombre de la bête désignait-il pendant le second conflit mondial ? Je vous le donne en mille. Eh oui, si A vaut 100, B 101, etc. « DCLXVI » se prénomme… Adolf.

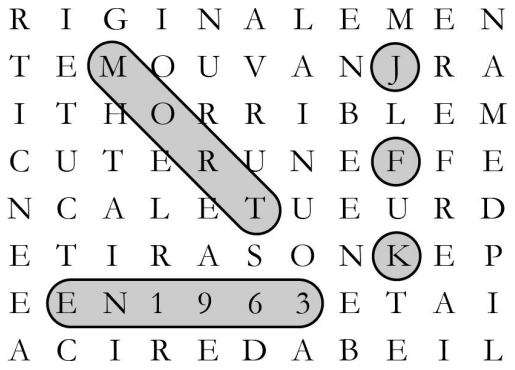
À condition de ne pas être pris au sérieux, l'occultisme peut être rangé dans les divertissements de l'esprit comme les mots croisés. Le lecteur intéressé pourra s'amuser à chercher la règle attribuant le nombre 666 au président actuel de la République française ou au roi des Belges. Modernité oblige, l'usage du code ASCII n'est pas interdit.

L'affaire se corse quand il se trouve des gens suffisamment crédules pour laisser influencer leur vie par de telles balivernes. Malgré ses qualités de mathématicien, Michael Stifel semblait croire à ses petits comptes. Il prophétisa ainsi la fin du monde pour le 3 octobre 1533. Apparemment, il était excellent prédicateur car, en prêchant

dans les campagnes, il réussit à convaincre de nombreux paysans de quitter leur terre. Rien ne se produisit le jour dit et Stifel dut se réfugier en prison pour échapper à la colère de ses adeptes. Nous aimerions pouvoir sourire de la naïveté de ces braves paysans si des exemples récents ne montraient pas le pouvoir de nuisance de ceux qui jouent avec la crédulité humaine. Heureusement, la fin du monde reste et restera toujours pour demain.

Le code de la Bible

Dernier avatar de cette quête désespérée de sens : le « code » de la Bible. Depuis quelques années, l'art ancien de la gématrie est dépassé par une façon nouvelle de découvrir des messages secrets dans le livre religieux. Un mathématicien israélien né en 1948 en Lettonie, Eliyahu Rips, y a trouvé un grand nombre de prédictions. Des prédictions du passé bien sûr : prédire le futur est toujours un exercice plus risqué ! Eliyahu Rips s'est en fait laissé aveugler par des mots qu'il pense avoir découverts à travers des lettres décalées de manière constante. Les mots originaux sont bien entendu en hébreu, mais voici quelques exemples en français :



Annonce de la mort de John Fitzgerald Kennedy dans le style du code de la Bible. La règle du décalage donne des motifs en colonnes, en lignes ou en diagonales. Le résultat n'est pas sans une certaine esthétique.

D’après l’étude d’Eliyahu Rips, la Bible fourmille de ce genre de prédictions. Pas moins de sept assassinats d’hommes d’État y seraient annoncés. S’agit-il vraiment de prophéties ? Le hasard peut-il être responsable de ces étranges messages dissimulés dans la Bible ? Certains pensent que c’est impossible et y voient la preuve de l’existence de Dieu, d’autres celles de l’intervention d’extraterrestres venus de la nuit des temps pour nous prévenir des dangers qui nous guettent… Examinons la règle utilisée par Rips : elle revient à constituer des textes en partant d’une lettre donnée de la Bible, la troisième par exemple, et en sautant toujours le même nombre de lettres, quatre par exemple. Avec cette règle, la phrase « la **m**ême h**o**nte a**r**rive **t**ôt ou tard » véhicule le mot « mort ».

Cela dit, le plus souvent, ces textes sont comme formés de lettres au hasard. Quelle est la probabilité d’y trouver un mot donné, comme « MORT » ? Pour étudier la question, imaginez un jeu de 26 cartes, notées de A à Z. Pensez à une lettre, A par exemple, puis tirez une lettre au hasard. Quelle est la probabilité que ce soit la lettre à laquelle vous pensiez ? Une sur 26 bien sûr, puisque chaque possibilité a la même chance de survenir. Recommençons avec deux lettres, en remettant la première tirée dans le jeu. La probabilité de tirer le mot choisi au hasard est maintenant d’une sur $26^2 = 26 \times 26 = 676$. Pour trois lettres, ce sera une sur $26^3 = 26 \times 26 \times 26 = 17\,576$ et ainsi de suite. Pour un mot de quatre lettres, on trouve une sur 456 976 et pour cinq, une sur 11 881 376, etc.

Si notre texte désordonné contient cent mille caractères, il y a donc une chance sur cinq que le mot « MORT » (quatre lettres) y figure. Il est donc presque impossible que le mot « MORT » ne se trouve pas quelque part dans la Bible… ou dans n’importe quel autre texte de longueur équivalente. Bien entendu, la probabilité devient réduite si on cherche des mots longs et des occurrences semblant annoncer la mort de tel ou tel homme célèbre, mais il est quasiment sûr

que des « prophéties » de ce type figurent dans bien des romans. De même, parmi un grand nombre de rochers, il est difficile de ne pas en trouver qui évoque un personnage célèbre, la reine Victoria dans les pays anglo-saxons, Louis XVI ou le général de Gaulle en France. De même, le rêveur verra apparaître toutes sortes de personnages, d'animaux ou d'objets dans le ciel. N'y voyez aucun présage. La seule origine de ces coïncidences est le hasard !

Le roman *Moby Dick* d'Herman Melville a été particulièrement étudié de ce point de vue, suite à un défi d'un journaliste convaincu de la réalité des prophéties découvertes par Rips : « Si ceux qui me critiquent arrivent à trouver dans *Moby Dick* un message codé annonçant la mort d'un premier ministre, je les croirai. » Comme de bien entendu, on en trouva sept dans le roman.

Ce Qu'il Faut Décrypter

Une prophétie dans *Moby Dick*

Ce passage de *Moby Dick* annonce la mort d'un premier ministre :

O R W I T H A W H I T E P
N A H A B Y O U N G M A N
K L E S H I S G R A N D D
D S Y E T I N G E N E R A
T H E B L O O D Y D E E D
E R M W H A L E S H E A D
T T O I M P O S S I B L E

Lequel ?

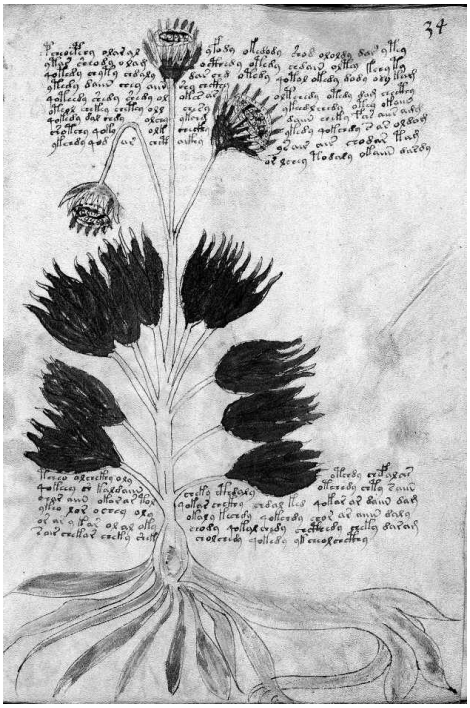
Bien avant qu'on ne cherche des messages codés dans la Bible, des apprentis cryptologues, dont Elizabeth Wells Gallup (1848-1934), avaient déniché des messages chiffrés dans les œuvres de Shakespeare, comme nous l'avions esquissé. Plus précisément, dans les parties en italiques de l'édition de 1623, où l'on peut distinguer des différences minimes dans le dessin des lettres. Mrs Gallup y a vu un message ayant été codé avec le chiffre inventé par Francis Bacon et en a déduit que le philosophe serait l'auteur des pièces de Shakespeare (et aussi le fils d'Elizabeth I^re^). En fait, les irrégularités constatées venaient des fontes d'imprimerie (des lettres en plomb) qui étaient mises à contribution jusqu'à usure complète.

Le manuscrit de Voynich

Pour finir ce chapitre sur les dérives cryptographiques, mentionnons un manuscrit dont nous ne prétendons pas qu'il soit pathologique, mais qui a suscité des interprétations méritant ce qualificatif. En 1912, Wilfrid Voynich (1865-1930), un antiquaire installé aux États-Unis, se rendit en Italie pour acheter des livres anciens que les jésuites vendaient pour restaurer l'une de leurs villas. Parmi ses achats figurait un manuscrit semblant dater du XIII^e^ siècle et rédigé dans une langue non déchiffrée à l'époque et qui ne l'est toujours pas aujourd'hui. Avec leurs ronds et leurs crochets qui paraissent s'envoler, les lettres de ce texte ressemblent à une écriture elfique tout droit sortie du *Seigneur des anneaux*. S'agit-il d'un herbier, d'un texte d'alchimie ou ésotérique ? Nous l'ignorons, mais surtout : le manuscrit de Voynich est-il un texte chiffré ?

Je serais tenté de le croire. L'examen du texte montre en effet des caractères à la mode des chiffreurs de l'époque, comme ceux du code de Philibert Babou ou de Marie Stuart, par exemple. En revanche, la graphie laisse penser que le

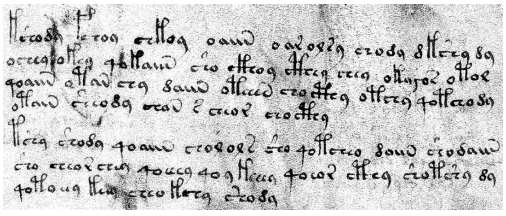
scribe comprenait ce qu'il écrivait, pour la simple et bonne raison qu'il n'y a aucun arrêt au milieu des mots. Le texte est écrit de gauche à droite puisque les paragraphes se terminent par un blanc à droite. Cette particularité exclut un chiffrement à la manière de Léonard de Vinci, qui écrivait ses missives confidentielles dans un miroir. Vu l'époque (selon des datations au carbone 14, son écriture remonterait plutôt au XV^{e} ou XVI^{e} siècle ; les illustrations correspondent d'ailleurs à ce que l'on faisait en Europe occidentale à cette époque), il est naturel de penser à une simple substitution, agrémentée de quelques mots codés. Les calculs de fréquence n'ont abouti à aucun résultat, hormis celui que le manuscrit présente davantage de répétitions que les langues ordinaires.



Le manuscrit de Voynich est très illustré et semble écrit dans une langue occidentale, les caractères utilisés étant proches des caractères latins. Le manuscrit comporte une lettre laissant entendre qu'il était l'œuvre du savant et alchimiste Roger Bacon (1214-1294). Le carbone 14, qui lui a attribué un âge plus tardif, suffit à démonter cette hypothèse.

Si le manuscrit était chiffré à partir d'une des langues connues de l'époque (latin, français, anglais, etc.), il aurait probablement été décrypté depuis, ce qui laisse trois hypothèses, dont deux qui se rejoignent. La première est qu'il s'agit d'un faux, fabriqué pour être vendu. L'auteur l'aurait donc écrit en « charabia » et ajouté des illustrations pour le vendre comme un livre d'alchimiste renfermant des secrets à découvrir. Si le texte n'avait que quelques pages, cette hypothèse serait vraisemblable ; or il en comporte 240. Ecrire un texte aussi long dans une langue sans véritable sens conduit presque fatalement à se répéter. Par ailleurs, les analyses de fréquences des mots ne confortent pas cette hypothèse.

Même si on ne peut exclure formellement cette possibilité, il semble plus probable que le texte ait été écrit dans une langue artificielle, qui serait alors une sorte de langue secrète des alchimistes de l'époque. La dernière hypothèse, très semblable, serait celle d'un jargon modifié au moyen de règles simples comme celles des argots, verlan, javanais ou autres. Les cryptologues qui se sont penchés sur le manuscrit ont tenté d'appliquer dessus la méthode du mot probable, en se fondant sur les noms des plantes illustrant le texte dans l'une de ses parties. Hélas, les plantes se sont révélées… imaginaires, ce qui milite en faveur d'un faux fabriqué de toutes pièces. Le mystère reste donc entier. Il est possible que le manuscrit de Voynich soit une énigme pour toujours, ou au moins tant que l'on ne saura pas dans quel contexte culturel particulier il a vu le jour.



Détail du manuscrit de Voynich.

8
Les substitutions à plusieurs alphabets

Nous voilà parvenus au second niveau de complexité des codes secrets. À partir de maintenant, les choses sérieuses commencent : munissez-vous d'un verre d'eau et d'un tube d'aspirine, vos neurones vont chauffer un peu ! Mais le jeu en vaut la chandelle, je vous assure, car ce chapitre nous sera nécessaire pour comprendre plus tard comment fonctionne la célèbre machine Enigma et comment son décryptement a grandement contribué à la victoire des Alliés pendant la Seconde Guerre mondiale. Rien que ça. L'Enigma est en effet l'héritière des améliorations apportées dès le XVIe siècle à l'une des grandes familles de chiffres que nous avons rencontrées.

Vous vous souvenez des chiffres à substitution dont l'archétype est le chiffre de César ? L'idée est de remplacer chaque lettre du message par une autre lettre puisée dans un alphabet différent. Comme nous l'avons vu, il est facile de casser ce type de codes en appliquant la méthode des fréquences d'Al-Kindi (quelle est la lettre la plus représentée dans le message ? La deuxième et ainsi de suite…). Pour contrecarrer cette attaque, on a inventé des substitutions homophones qui mobilisent plusieurs chiffrements pour les lettres fréquentes, mais sans régler pour autant le problème car ces chiffres ne résistent pas longtemps à la technique du mot probable.

À la Renaissance, conscients des limites de ces codes, plusieurs cryptologues ripostèrent en imaginant des systèmes où la substitution est modifiée selon la place de la lettre dans le message.

Le premier chiffre à mot-clef

Pour éviter le décryptement par la méthode des fréquences, Jean Trithème, que nous avons déjà rencontré à propos de ses litanies, a imaginé de décaler chaque lettre du message de 0, puis de 1, puis de 2, etc. lettres. Ainsi « ATTAQUE » se chiffre en « AUVDUZK » (A est conservé, T changé en U, le second T en V, etc.). Aussi astucieux qu'il soit, ce chiffrement a l'immense défaut de ne pas dépendre d'une clef. Autrement dit, une fois la méthode découverte, il est facile de décrypter tous les messages ainsi chiffrés.

Ce Qu'il Faut Décrypter

Un message en Trithème

On intercepte le message suivant :

LFEKM KLYMM OEDVH WUDWX MOBXG ALFED VNRUM MOAQA REQJV NHZYI CE

Saurez-vous le décrypter ?

Giovan Bellaso, né en 1505 à Brescia (et mort à une date inconnue), semble le premier à avoir eu l'idée de sécuriser un chiffre à l'aide d'un mot-clef – une expression à prendre au sens littéral ici. Son code est un chiffre poly-alphabétique très proche du chiffre de Vigenère, que nous décrirons plus loin. Bellaso décrit son système dans un ouvrage paru en 1553, *La Cifra del Sig. Giovan Battista Bellaso*. Il utilise cinq

alphabets réversibles, comportant chacun 20 lettres (comme c'était toujours le cas à son époque, les lettres I, J et Y sont confondues tout comme U, V et W ; K et Z sont absents) et construits à partir d'un mot-clef, « VITE » dans l'exemple que nous donnons. Voici le premier alphabet :

V	I	A	B	C	D	F	G	H	L
T	E	M	N	O	P	Q	R	S	X

La règle de construction de Bellaso est simple : on écrit d'abord le mot-clef sur deux lignes et on complète la première ligne par les lettres non utilisées dans l'ordre, puis on fait de même pour la seconde ligne. Pour construire les quatre alphabets suivants, on décale d'un cran vers la droite la seconde ligne. Voici le deuxième alphabet :

V	I	A	B	C	D	F	G	H	L
X	T	E	M	N	O	P	Q	R	S

Les trois autres suivent. On étiquette alors ces alphabets en écrivant verticalement le premier alphabet de gauche à droite et de haut en bas.

VDTP	V	I	A	B	C	D	F	G	H	L	
		T	E	M	N	O	P	Q	R	S	X
IFEQ	V	I	A	B	C	D	F	G	H	L	
		X	T	E	M	N	O	P	Q	R	S
AGMR	V	I	A	B	C	D	F	G	H	L	
		S	X	T	E	M	N	O	P	Q	R
BHNS	V	I	A	B	C	D	F	G	H	L	
		R	S	X	T	E	M	N	O	P	Q

CLOX	V	I	A	B	C	D	F	G	H	L	
		Q	R	S	X	T	E	M	N	O	P

Un autre mot-clef est nécessaire pour chiffrer, par exemple « DEPVIS ». Pour chiffrer un message comme « Le chiffre de Bellaso est poly-alphabétique ». On l'écrit mot par mot dans un tableau avec le mot-clef, en n'utilisant que les lettres de l'alphabet, bien entendu :

Clair	LE	CHIFFRE	DE	BELLASO	EST	POLI	ALPHABETIQVE
Clef	D	E	P	V	I	S	D
Chiffré	XI	NRTPPHA	PI	NIXXMHC	ALI	HGQS	MXDSMNIVEFTI

La version chiffrée est donc :

XI NRTPPHA PI NIXXMHC ALI HGQS MXDSMNIVEFTI

Ce Qu'il Faut Décrypter

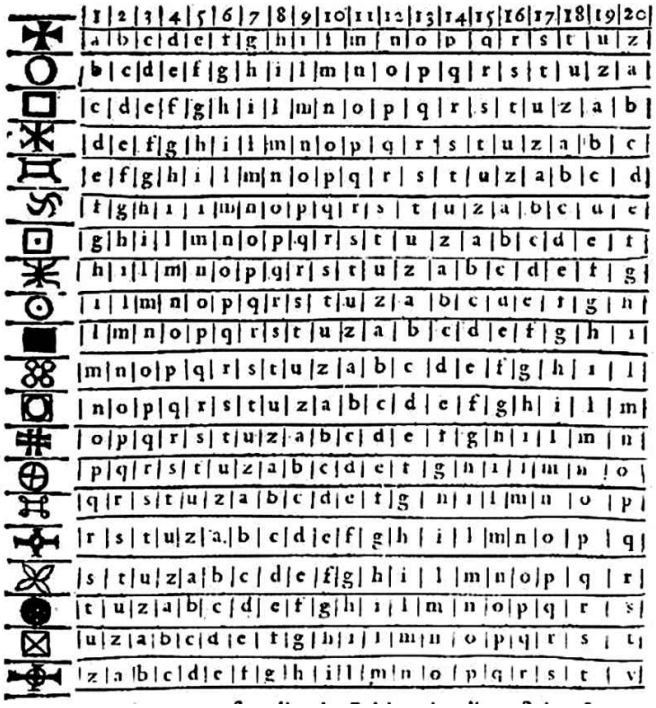
Un message en Bellaso

On intercepte le message suivant :

QV QFBHOIH OA TOGSHXNF BIA AG DQSRBFHSQT

On sait qu'il a été chiffré en Bellaso avec les clefs RATE et CORDE.
Que signifie-t-il ?

En 1734, José de Gronsfeld modifia les chiffres de ce type en se contentant de simples décalages de César pour chaque substitution. Une remarque : si les ouvrages lui en attribuent souvent la paternité, cette simplification se trouve cependant déjà en 1563 dans l'ouvrage *De furtivis literarum notis* de Giambattista Della Porta, le cryptologue que nous avons déjà cotoyé à propos de la méthode du mot probable. Reprenant une vieille tradition, la table de Della Porta s'accompagne de symboles alchimiques (voir page suivante).



Sur cette page du livre de Della Porta, les alphabets sont décalés d'un cran à chaque ligne, ce qui correspond à une utilisation moderne du chiffrement de Vigenère. Ces alphabets sont indiqués dans la colonne de gauche par des signes alchimistes.

Si de nombreux cryptologues, comme Bellaso ou Della Porta, ont proposé des chiffres de substitution poly-alphabétiques, l'Histoire a retenu Blaise de Vigenère (1523-1596) comme inventeur de la méthode. Vigenère n'a jamais prétendu en être le père, mais il écrivit un traité si clair à son propos que c'est probablement la raison qui poussa à lui tresser des lauriers.

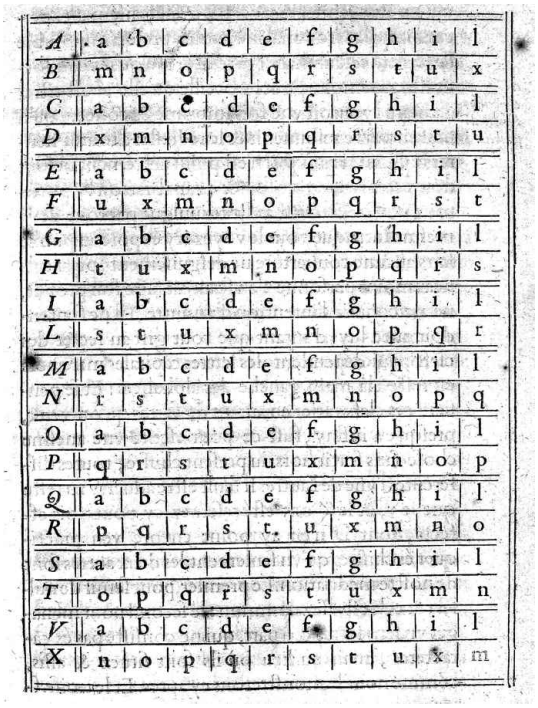
Blaise de Vigenère, un personnage multiple

Personnage foisonnant, Blaise de Vigenère semble avoir vécu plusieurs vies. Expert en cryptologie, alchimiste et kabbaliste, il a été également écrivain et traducteur. Il savait lire cinq ou six langues dont le latin, le grec et l'hébreu. Pour couronner le tout, c'était un diplomate qui, au

service des ducs de Nevers et des rois de France, a parcouru les chemins d'une Europe particulièrement agitée à son époque. En résumé un esprit de la Renaissance, curieux de tout et, en premier lieu, de ce qui n'est pas offert à nos yeux de façon évidente. Ce qui le destinait donc à devenir maître dans l'art du secret…

Le chiffre de Vigenère original porte sur vingt lettres car il confond les lettres I, J et Y d'un côté, les lettres V et W de l'autre et il omet Z. Il part alors de dix substitutions qu'il nomme alphabets. Elles sont rassemblées dans un tableau (voir la figure p. suivante). Il dispose ainsi de dix alphabets réversibles, nommés chacun par deux lettres majuscules. Les substitutions se lisent directement dans chaque ligne. Ainsi, l'alphabet A (et B) échange les lettres a et m, b et n, etc. Vigenère décrit le fonctionnement de son code dans son *Traicté des chiffres, ou Secrètes manières d'escrire* paru en 1586 :

> Prenons donc qu'on veuille représenter le sujet : « au nom de l'éternel soit mon commencement » au moyen de cette table ; et que la clef du chiffre soit « le jour obscur » […] vous procéderez de la sorte. Cherchez en la colonne des capitales, la lettre L, qui est la première de notre clef, et voyez quelle lettre correspond en son alphabet à celle de A, la première aussi du sujet ; ce sera S. Poursuivez ainsi de lettre en lettre tant que la clef se pourra étendre ; Puis étant au bout vous la réitérerez de nouveau : u de e, donne a: n de i, f: o de o, h: m de u, l: d de r, s: e de o, u: l de b, x: e de s, s: t de c, i: e de u, r: r de r c: n l de f: e de e, o: l de i, r: s de o, c: o de u, b: i de r, n: t de o d: m de b, a: o de s, l: n de c, c: c de u, p: o de r, l: m de l, e: m de e, c: c de i, s: n de o, g: e de u, p: e de r, t: m de o, g: e de b, q: n de s, i: t de c, i. Ajoutez-y ces quatre lettres au-devant pour perdues, et ne servant à rien qu'à embrouiller : d r g q et insérez au bout de chaque mot l'une des deux gardées pour mille, à savoir y et z pour les distinguer l'un de l'autre, votre contexte sur cette clef « Le jour obscur » pour ce premier vers, au nom de l'éternel soit mon commencement, sera tel : d r g q s a y f h l z s u y x s i r c f o r z o b n d y a l c z p l e c s g p t g q i i y.



A	a	b	c	d	e	f	g	h	i	l
B	m	n	o	p	q	r	s	t	u	x
C	a	b	c	d	e	f	g	h	i	l
D	x	m	n	o	p	q	r	s	t	u
E	a	b	c	d	e	f	g	h	i	l
F	u	x	m	n	o	p	q	r	s	t
G	a	b	c	d	e	f	g	h	i	l
H	t	u	x	m	n	o	p	q	r	s
I	a	b	c	d	e	f	g	h	i	l
L	s	t	u	x	m	n	o	p	q	r
M	a	b	c	d	e	f	g	h	i	l
N	r	s	t	u	x	m	n	o	p	q
O	a	b	c	d	e	f	g	h	i	l
P	q	r	s	t	u	x	m	n	o	p
Q	a	b	c	d	e	f	g	h	i	l
R	p	q	r	s	t	u	x	m	n	o
S	a	b	c	d	e	f	g	h	i	l
T	o	p	q	r	s	t	u	x	m	n
V	a	b	c	d	e	f	g	h	i	l
X	n	o	p	q	r	s	t	u	x	m

Extrait du *Traicté des chiffres, ou Secrètes manières d'escrire* de Blaise de Vigenère (1586). Les alphabets de Vigenère sont désignés par une lettre majuscule (première colonne). Pour l'alphabet A, *a* et *m* sont échangés ainsi que *b* et *n*, etc. Il s'agit d'alphabets réversibles.

Le chiffre décrit par Vigenère possède des complications inutiles, certaines mêmes nocives. Il est inutile en effet d'utiliser des substitutions mono-alphabétiques plus sophistiquées que le décalage de César, car elles sont cassables presque aussi facilement que celui-ci et vulnérables à l'espionnage. Si, pour la même raison, l'ajout des quatre lettres ne sert pas à grand-chose, celui des lettres *y* ou *z* en fin de mots est pour le moins malvenu. Dans le cas où le secret est percé, ce signe distinctif facilite la tâche des déchiffreurs pour découper les mots…

Ces raisons ont poussé les cryptologues à épurer le chiffre de Vigenère. De nos jours, le code correspond à un décalage variant selon la lettre utilisée. La clef est encodée dans un mot ou un texte. Voyons comment le code fonctionne avec le message « le chiffre de Vigenère est un César à décalage variable » et la clef « abbé ». On écrit d'abord le message

dans un tableau sans espace ni ponctuation avec la clef en dessous, en la répétant autant de fois que nécessaire. Le décalage dépend du numéro d'ordre de la lettre considérée, 0 pour A, 1 pour B et 4 pour E. On applique alors le décalage indiqué sous chaque lettre du message.

L	E	C	H	I	F	F	R	E	D	E	V
A	B	B	E	A	B	B	E	A	B	B	E
0	1	1	4	0	1	1	4	0	1	1	4
L	F	D	L	I	G	G	V	E	E	F	Z

I	G	E	N	E	R	E	E	S	T	U	N
A	B	B	E	A	B	B	E	A	B	B	E
0	1	1	4	0	1	1	4	0	1	1	4
I	H	F	R	E	S	F	I	S	U	V	R

C	E	S	A	R	A	D	E	C	A	L	A
A	B	B	E	A	B	B	E	A	B	B	E
0	1	1	4	0	1	1	4	0	1	1	4
C	F	T	E	R	B	E	I	C	B	M	E

G	E	V	A	R	I	A	B	L	E
A	B	B	E	A	B	B	E	A	B
0	1	1	4	0	1	1	4	0	1
G	F	W	E	R	J	B	F	L	F

Chiffrement de Vigenère moderne. Le chiffre de Gronsfeld est identique, mais la clef est donnée sous la forme d'une liste de chiffres, 0114 ici, au lieu d'un mot comme « abbé ».

Le chiffrement est plutôt laborieux, puisqu'il faut décaler chaque lettre de façon distincte, ce qui explique que la méthode ait été pratiquement ignorée pendant près de trois siècles. Il faut dire que la moindre erreur pouvait rendre le message indéchiffrable pour son destinataire !

Table de Vigenère

Pour adopter la version moderne du chiffre de Vigenère, on peut s'aider d'une table donnant le message chiffré plus facilement à partir de la clef (voir ci-dessous). C'est en fait une table de Pythagore (tableau qui aide à retrouver le résultat d'une opération élémentaire comme l'addition ou la multiplication) pour l'opération de chiffrement. Si la lettre à chiffrer est H et que la clef est X, on lit le résultat à l'intersection de la colonne H et de la ligne X (ou le contraire, puisque l'opération est symétrique). On trouve E.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Table de chiffrement pour la version moderne du chiffre de Vigenère.

Il s'agit d'une opération qu'on peut noter additivement : chiffré = clair + clef, l'addition se faisant modulo 26 comme

nous l'avons déjà vu à propos du chiffre de Hill (voir le chapitre 4). Cette façon de noter l'opération de chiffrement revient à confondre A et 0, B et 1, … Z et 25, puis à remplacer le résultat par son reste dans la division par 26. Ainsi, V + E = Z comme 21 + 4 = 25 et T + U = N comme 19 + 20 = 39 = 13 modulo 26.

Le chiffre de Beaufort

L'amiral anglais Francis Beaufort (1774-1857), plus connu pour son invention de l'échelle mesurant la force du vent en fonction de l'aspect de la mer, utilisait pour ses affaires personnelles un chiffre fondé sur la table de chiffrement de Vigenère. Plus précisément, pour chiffrer L avec la clef C, il repérait L sur la première ligne de la table, descendait alors dans la colonne jusqu'à trouver la clef C, enfin il suivait la ligne obtenue jusqu'à la première colonne : le chiffré était là. Il s'agit de R. L'opération peut s'écrire : chiffré = clef – clair. Voici l'exemple du chiffrement de l'expression « le chiffre » avec la clef « car » :

L	E	C	H	I	F	F	R	E
C	A	R	C	A	R	C	A	R
R	W	P	V	S	M	X	J	N

Chiffrement de Beaufort.

Le chiffre de Beaufort admet une variante dite à l'allemande, où on retranche la clef au clair, soit chiffré = clair – clef. Pour décrypter un message chiffré en Vigenère, il suffit d'y appliquer la variante allemande de Beaufort avec la même clef. Autrement dit, chiffrer en Vigenère équivaut à déchiffrer en la variante allemande de Beaufort et vice versa.

Une complication illusoire : le chiffre de Rozier

Le chiffre de Rozier se fonde également sur la table de Vigenère. Pour chiffrer L avec la clef C, on repère L sur la

première ligne de la table et on descend sur la colonne jusqu'à trouver la clef C, puis on continue sur la ligne de C jusqu'à trouver la lettre suivante de la clef, soit D. On remonte alors jusqu'à la première ligne : le chiffré est là.

Voici l'exemple du chiffrement de l'expression « le chiffre » avec la clef « car » :

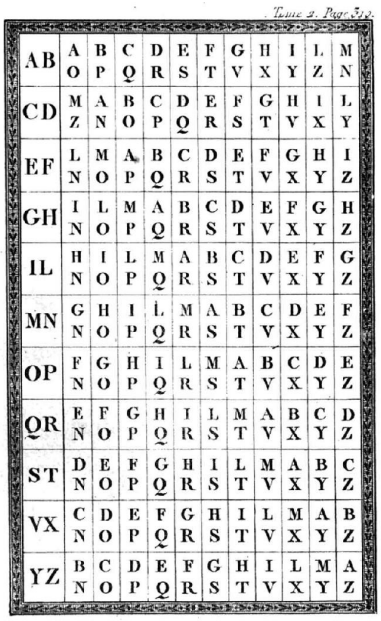
L	E	C	H	I	F	F	R	E
C	A	R	C	A	R	C	A	R
J	V	N	F	Z	Q	D	I	P

Chiffrement de Rozier.

On remarque facilement que le même chiffré est obtenu avec la méthode de Vigenère et la clef YRL. Ce résultat est général : le chiffre de Rozier équivaut au chiffre de Vigenère, seule la clef change.

Les lettres de Marie-Antoinette

Marie-Antoinette chiffrait ses lettres par substitution poly-alphabétique. Pour ce faire, elle disposait d'une table de chiffrement par destinataire. Nous en proposons une page suivante.



Tome 2. Page 312.

AB	A O	B P	C Q	D R	E S	F T	G V	H X	I Y	L Z	M N
CD	M Z	A N	B O	C P	D Q	E R	F S	G T	H V	I X	L Y
EF	L N	M O	A P	B Q	C R	D S	E T	F V	G X	H Y	I Z
GH	I N	L O	M P	A Q	B R	C S	D T	E V	F X	G Y	H Z
IL	H N	I O	L P	M Q	A R	B S	C T	D V	E X	F Y	G Z
MN	G N	H O	I P	L Q	M R	A S	B T	C V	D X	E Y	F Z
OP	F N	G O	H P	I Q	L R	M S	A T	B V	C X	D Y	E Z
QR	E N	F O	G P	H Q	I R	L S	M T	A V	B X	C Y	D Z
ST	D N	E O	F P	G Q	H R	I S	L T	M V	A X	B Y	C Z
VX	C N	D O	E P	F Q	G R	H S	I T	L V	M X	A Y	B Z
YZ	B N	C O	D P	E Q	F R	G S	H T	I V	L X	M Y	A Z

CHIFFRE
DE S. M. MARIE ANTOINETTE,
Reine de France.

Un des tableaux de chiffrement de Marie-Antoinette.

On notera que ce tableau ne contient que 22 lettres, les lettres manquantes sont J, K, U et W, ce qui correspond à l'usage venant du latin que nous avons déjà rencontré, où I et J d'un côté, U et V de l'autre sont confondues. K peut être remplacé par C et W par V.

Clef de chiffrement

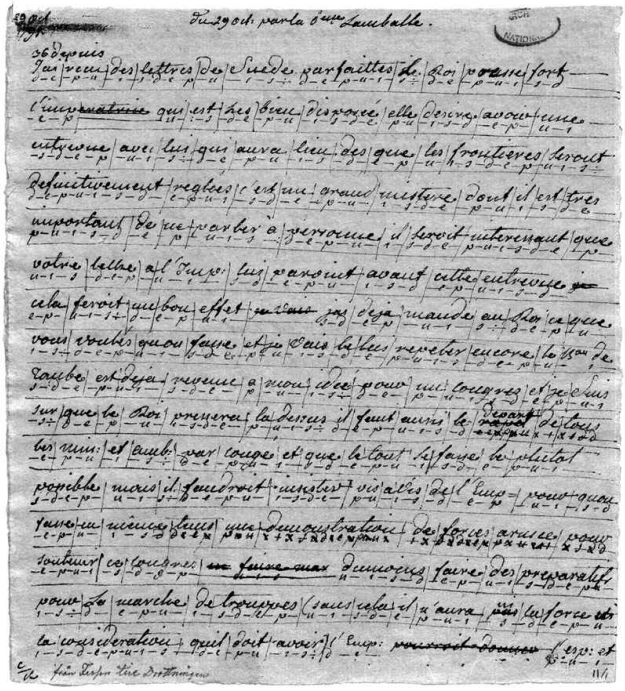
Comme nous l'avons déjà noté, l'utilisation de cette table pour chiffrer demande une clef secrète qu'on partage avec le destinataire. Par exemple, si la clef est « sel », pour chiffrer la première lettre, on utilise la ligne dont la première colonne est ST. D est alors changé en N (et N en D), E en O, etc. Pour chiffrer la seconde, on utilise la ligne dont la première colonne est EF. Pour chiffrer une phrase comme « je vous aime », construisons un tableau à 10 lignes et 3 colonnes :

J	E	V	O	U	S	A	I	M	E
S	E	L	S	E	L	S	E	L	S
S	T	D	E	F	B	X	Z	Q	O

Le message chiffré est donc « stdefbxzqo ». Si vous essayez de chiffrer une lettre ainsi, vous verrez la difficulté d'éviter les erreurs. Pour cette raison, un cryptologue inconnu avait conseillé à Marie-Antoinette de ne chiffrer qu'une lettre sur deux ce qui, en fournissant des repères, simplifie grandement le chiffrement mais l'affaiblit tout aussi grandement. Voici pourquoi. Le tableau devient :

J	E	V	O	U	S	A	I	M	E
	S		E		L		S		E
J	O	V	M	U	B	A	S	M	T

Le message chiffré est maintenant « jovmubasmt ». On peut examiner des lettres ainsi chiffrées par Marie-Antoinette aux Archives nationales (p. suivante).



Travail de chiffrement d'une lettre envoyée au comte de Fersen – où l'on voit que Marie-Antoinette ne chiffrait qu'une lettre sur deux.

Le décryptement sans connaître la clef est ainsi facilité, surtout si on connaît le tableau de chiffrement. C'est ici que des talents de cruciverbiste sont utiles. En effet, on peut deviner un mot si on en connaît une lettre sur deux, comme ici « J-V-U-A-M », qui est transparent pour tout amateur de mots croisés (on reconnaît le texte : « Je VoUs AiMe »). Ensuite, on sait que la première lettre de la clef transforme E en O, ce qui ne se produit que pour ST. En continuant ainsi, on décrypte le message quelle que soit sa longueur.

Une telle façon de procéder favorise la méthode du mot probable. Pour préciser la façon de s'y prendre, prenons un exemple sans table de chiffrement, en employant un décalage variable. Considérons le message suivant :

CEVOO EFTEU GLYSS AYMER ZEENZ OVNIT KE

Imaginons que nous pensions y débusquer le nom « Marie-Antoinette ». Pour décrypter la phrase, faisons défiler ce terme le long du message jusqu'à trouver une

coïncidence d'une lettre sur deux. Nous la découvrons à la fin.

M	E	R	Z	E	E	N	Z	O	V	N	I	T	K	E
M	A	R	I	E	A	N	T	O	I	N	E	T	T	E

Découverte du mot probable

Cela signifie que « AIATIET » est chiffré en « EZEZVIK ». Comptons les décalages nécessaires pour aboutir à cette correspondance. Nous obtenons alors les lettres de la clef : « EREGNER ». Celle-ci est donc probablement « REGNE ». Le message est facile à décrypter, il signifie : « Le roi est au plus mal. Marie-Antoinette ». Bien entendu, nous avons ignoré la table de chiffrement pour simplifier notre démonstration, mais elle ne rend pas le décryptement bien plus difficile.

Marie-Antoinette de Habsbourg (1755-1793). Portrait d'Élisabeth Vigée-Lebrun.

La méthode de chiffrement de Marie-Antoinette n'était guère sûre. Cela n'eut aucune conséquence funeste pour elle car le tribunal révolutionnaire ne se fatigua pas à faire décrypter ses lettres. Son procureur, le tristement célèbre Fouquier-Tinville, n'avait besoin d'aucune preuve pour envoyer les gens à la guillotine. Son sort était scellé de toute façon et elle aurait pu s'épargner ce travail pénible de chiffrement dont elle se plaint dans une lettre au comte de Fersen datée du 2 novembre 1791 :

> Adieu, je suis fatiguée à force d'écritures ; jamais je n'ai fait tel métier, et je crains toujours d'oublier, ou de mettre quelques bêtises.

La faiblesse du chiffre de Marie-Antoinette fait que nous savons très bien de nos jours décrypter les lettres envoyées par la reine. Pourtant, dans les textes parus chez l'éditeur de fonds historiques Paleo, les passages montrant la nature de l'affection que Marie-Antoinette portait au comte de Fersen sont remplacés par de petits points, comme si elles étaient indécryptables. Ces parties ont été rétablies par Jacques Patarin et Valérie Nachef, deux cryptologues de l'université de Versailles… à l'aide de la même clef utilisée pour le reste de la lettre, le mot « depuis ». Il est étonnant que, de nos jours, on traite encore cette question comme un secret d'État ! Voici un passage assez clair d'une lettre datée du 29 juin 1791, toujours destinée au comte, et rétabli par décryptement :

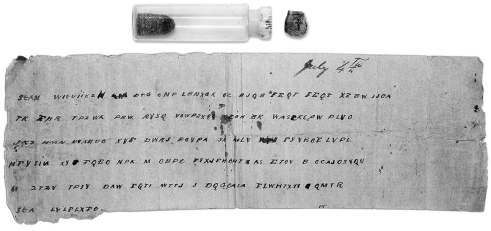
> J'existe mon bien aimé et c'est pour vous adorer. Que j'ai été bien inquiète de vous, et que je vous plains de tout ce que vous souffrez de n'avoir point de nos nouvelles. Le ciel permettra que celle-ci vous arrive. Ne m'écrivez pas, ce serait nous exposer, et surtout ne revenez pas ici sous aucun prétexte. On sait que c'est vous qui nous avez fait sortir d'ici ; tout serait perdu si vous paraissiez. Nous sommes gardés à vue jour et nuit ; cela m'est égal. Vous n'êtes pas ici. Soyez tranquille, il ne m'arrivera rien. L'Assemblée veut nous traiter avec douceur. Adieu le plus aimé des hommes. Calmez-vous si vous pouvez. Ménagez-vous pour moi. Je ne pourrais plus vous écrire mais rien au monde ne pourra m'empêcher de vous adorer jusqu'à la mort.

L'exemple de Marie-Antoinette montre pourquoi le chiffrement de Vigenère ne fut guère usité avant l'époque des communications rapides : une erreur était trop facile à commettre, le message devenant incompréhensible.

L’invention du télégraphe rendit le chiffre de Vigenère plus opérationnel. En cas d’erreur, le destinataire pouvait toujours demander à l’expéditeur de lui renvoyer une nouvelle version du message. On a alors imaginé des dispositifs mécaniques pour simplifier le chiffrement : ainsi débuta l’ère du chiffrement avec des machines (voir le chapitre 10).

Les erreurs de protocole des sudistes

Pendant la guerre de Sécession, les sudistes firent usage du chiffre de Vigenère. Pour l’époque, c’était encore un bon choix. Malheureusement pour eux, ils commirent au moins quatre erreurs de protocole. À cette occasion, nous allons découvrir que la manière d’appliquer un code pouvait être plus importante que le code lui-même. La pire des erreurs a été sans aucun doute qu’ils n’eurent jamais que trois clefs : « Manchester Bluff » et « Complete Victory » au début de la guerre et le surréaliste « Come Retribution » à la fin. Or, plus on collecte de messages chiffrés de manière identique, plus il est facile de les décrypter. La moindre prudence aurait été d’en changer chaque semaine. De plus, ils gardaient le découpage des mots !



Un message sudiste en Vigenère trouvé dans une bouteille dans le Mississippi, 147 ans après y avoir été jetée (le 4 juillet 1863). On remarque que la longueur des mots a été respectée, ce qui facilite le décryptement en cas d’interception. Ici, la clef de chiffrement est « Manchester Bluff ».

Ce Qu’il Faut Décrypter

Un message sudiste

Le message sudiste en Vigenère de la figure ci-dessus est :

SEAN WIEUIIUZH DTG CNP LBHXGK OZ BJQB FEQT XZBW JJOY TK FHR TPZWK PVU RYSQ VOUPZXGG OEPH CK UASFKIPW PLVO JIZ HMN NVAEUD XYF DURJ BOVPA SF MLV FYYRDE LVPL MFYSIN XY FQEO NPK M OBPC FYXJFHOHT AS ETOV B OCAJDSVQU M ZTZV TPHY DAU FQTI UTTJ J DOGOAIA FLWHTXTI QLTR SEA LVLFLXFO

Saurez-vous le décrypter ?

De plus, les sudistes transmettaient souvent une partie de leur message en clair et ne chiffraient que ce qu'ils voulaient garder secret. Une telle façon de faire favorise la méthode des mots probables, puisque l'intercepteur connaît le sujet précis du message : il lui reste à jouer aux devinettes ! La quatrième erreur concerne leur utilisation du télégraphe. Parfois, une lettre disparaissait et le message devenait incompréhensible. Il arrivait ainsi que les sudistes ne soient pas capables de déchiffrer leurs propres messages, comme le montre une anecdote où, après douze heures d'essais infructueux, le major Cunningham de l'armée d'Edmund Kirby Smith dut aller chercher l'original du message à cheval. Si l'erreur était due à la perte d'une lettre, elle était pourtant facile à rectifier puisque le message devait être compréhensible jusqu'à cet oubli. Il suffisait donc de décaler la clef à ce moment. Imaginons par exemple que le message du paragraphe sur Vigenère (p. 208) soit transmis avec la perte d'une lettre. Le destinataire reçoit :

LFDLI GGVEE FZIHF RESFI UVRCF TERBE ICBME GFWER JBFLF

Il le déchiffre avec la clef « ABBE » en disposant les lettres en tableau.

L	F	D	L	I	G	G	V	E	E	F	Z	I

A	B	B	E	A	B	B	E	A	B	B	E	A
0	1	1	4	0	1	1	4	0	1	1	4	0
L	E	C	H	I	F	F	R	E	D	E	V	I
H	F	R	E	S	F	I	U	V	R	C	F	T
B	B	E	A	B	B	E	A	B	B	E	A	B
1	1	4	0	1	1	4	0	1	1	4	0	1
G	E	N	E	R	E	E	U	U	Q	Y	F	S
E	R	B	E	I	C	B	M	E	G	F	W	E
B	E	A	B	B	E	A	B	B	E	A	B	B
1	4	0	1	1	4	0	1	1	4	0	1	1
D	N	B	D	H	Y	B	L	D	C	F	V	D
R	J	B	F	L	F							
E	A	B	B	E	A							
4	0	1	1	4	0							
N	J	A	E	H	F							

Déchiffrement avec une lettre manquante.

Le message perd tout sens après le mot « Vigenère ». En sautant la lettre suivante, cela ne donne rien. On saute donc celle qui suit.

L	F	D	L	I	G	G	V	E	E	F	Z	I
A	B	B	E	A	B	B	E	A	B	B	E	A
0	1	1	4	0	1	1	4	0	1	1	4	0
L	E	C	H	I	F	F	R	E	D	E	V	I

H	F	R	E	S	F	I		U	V	R	C	F
B	B	E	A	B	B	E	A	B	B	E	A	B
1	1	4	0	1	1	4	0	1	1	4	0	1
G	E	N	E	R	E	E		T	U	N	C	E
T	E	R	B	E	I	C	B	M	E	G	F	W
B	E	A	B	B	E	A	B	B	E	A	B	B
1	4	0	1	1	4	0	1	1	4	0	1	1
S	A	R	A	D	E	C	A	L	A	G	E	V
E	R	J	B	F	L	F						
E	A	B	B	E	A	B						
4	0	1	1	4	0	1						
A	R	I	A	B	L	E						

Déchiffrement en sautant une lettre.

Nous retrouvons maintenant le message : « Le chiffre de Vigenère e-t un César à décalage variable ». Il est facile de rétablir la lettre manquante « s ».

Le mot probable de Jules Verne

Jules Verne nous a déjà servi à illustrer le chapitre précédent. Le revoici avec le code secret qui est au centre de l’intrigue de *La Jangada* paru en 1881, chiffré avec la méthode de Vigenère :

Phyjslyddqfdzxgasgzzqqehxgkfndrxujugiocytdxvksbxhhuypodvyrymhuhpuydk
joxphetozsletnpmvffovpdpajxhyynojyggaymeynfuqlnmvlyfgsuzmqiztlbqgyugs
qeubvnrcredgruzblrmxyuhqhpdrrgcrohepqxufivvrplphonthvddqfhqsntzhhhnfe
pmqkyuuexktoggkyuumfvijdqdpzjqsykrplxhxqrymvklohhhotozvdksppsuvjhd

Le héros de Jules Verne le décrypte en supposant que son auteur l'a signé de son nom, Ortega. Les six dernières lettres du message étant « suvjhd », il suppose que « ortega » est devenu « suvjhd » et donc que la clef correspond à la suite de décalages 432513. En l'appliquant, il trouve un message cohérent, à condition de ne pas compter la lettre W.

Le message peut également être décrypté avec la méthode de Kasiski, que nous verrons plus loin, ou celle de l'indice de coïncidence (voir *Les coïncidences de Friedman*, p. 244), ce que fit probablement un élève de l'École polytechnique nommé Saumaire qui réussit à décrypter le message avant d'en avoir la solution dans le livre, qui paraissait alors en feuilleton. Dans ses mémoires, le mathématicien Maurice d'Ocagne raconte que Jules Verne serait venu se faire expliquer la méthode par son jeune lecteur…

Le héros de Jules Verne a eu la chance – celle que lui organisa son créateur. De fait, nous verrons plus loin que la méthode du mot probable est applicable sans avoir recours à la bonne fortune (voir *Le mot probable de Bazeries*, p. 238) et qu'il existe une méthode très simple dès lors qu'on dispose d'un grand nombre de messages chiffrés avec la même clef (voir *La méthode de Kerckhoffs*, p. 227).

L'autoclave de Cardan

Non, l'autoclave de Cardan n'est pas un instrument pour cuire les aliments, mais une façon de communiquer la clef de chiffrement dans le message chiffré lui-même, *clavis* étant le mot latin signifiant « clef ». Jérôme Cardan, déjà rencontré à propos de ses grilles, est à l'origine de cette

idée qu'il n'a malheureusement pas su développer correctement. Le concept était déjà à l'œuvre, quoique de façon non explicite, dans l'usage qu'Alberti proposait de son cadran (voir le chapitre 10). Le nom de Cardan lui est cependant resté attaché. La méthode nécessite une première clef, par exemple « CUIT », le reste de la clef étant le message en clair. Chiffrer un texte se fait comme pour un Vigenère ! En guise d'exemple, chiffrons le texte : « la clef est dans le texte ». On construit le tableau :

L	A	C	L	E	F	E	S	T	D
C	U	I	T	L	A	C	L	E	F
N	U	K	E	P	F	G	D	X	I
A	N	S	L	E	T	E	X	T	E
E	S	T	D	A	N	S	L	E	T
E	F	L	O	E	G	W	I	X	X

Le chiffré est donc « NUKEP FGDXI EFLOE GWIXX ». Le déchiffrement s'effectue comme pour un texte chiffré en Vigenère, mais progressivement. On commence par déchiffrer « NUKE » avec la clef CUIT, ce qui donne le début du texte clair « LACL » et donc la suite de la clef. On déchiffre « PFGD » avec la clef LACL et ainsi de suite. Si l'adversaire ne connaît pas la méthode, le décryptement est très délicat ; sinon, la solidité du chiffre se limite à celle de la vraie clef, CUIT ici. La méthode fonctionne pour des échanges de messages à petite échelle, mais ne convient pas à un usage intensif.

Les espions allemands et le chiffre du livre

Pendant la Seconde Guerre mondiale, plusieurs réseaux d'espionnage allemands se fièrent au chiffre de Vigenère. Le principe est bien décrit dans *Le Code Rebecca*, de Ken Follett. Chaque espion est muni d'un livre (*Le Livre de San Michele* d'Axel Munthe dans la réalité, *Rebecca*, de Daphne du Maurier dans la fiction) qui lui sert de recueil de clefs. Son correspondant a bien entendu le même, dans la même édition. La règle pour obtenir la clef est tout à la fois complexe et relativement simple à retenir. L'espion utilise son numéro personnel auquel il ajoute huit fois le numéro du mois, ce qui détermine la page du livre où se trouve la clef. Ken Follett complique cette clef en supprimant un mot sur 5 si on est au mois de mai, 6 si on est en juin, etc. Si la clef choisie est aussi longue qu'une page d'un livre, ce code reste difficile à décrypter. Cependant, il a le gros inconvénient de reposer sur le secret et contrevient ainsi au principe de Kerckhoffs.

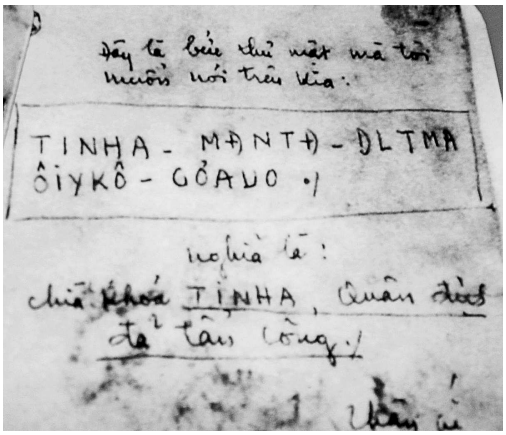
Cette idée de se munir d'un livre pour chiffrer remonte aux débuts de l'imprimerie. Deux personnes désirant communiquer de manière secrète peuvent choisir un texte se trouvant dans un livre qu'ils partagent. Partons du message « Si le Livre de San Michele s'est trouvé devenir une autobiographie, c'est que la manière la plus simple d'écrire sur soi-même consiste à s'efforcer de penser à d'autres ». Numérotons les mots dans l'ordre :

1 Si, 2 le, 3 Livre, 4 de, 5 San, 6 Michele, 7 s, 8 est, 9 trouvé, 10 devenir, 11 une, 12 autobiographie, 13 c, 14 est, 15 que, 16 la, 17 manière, 18 la, 19 plus, 20 simple, 21 d, 22 écrire, 23 sur, 24 soi, 25 même, 26 consiste, 27 à, 28 s, 29 efforcer, 30 de, 31 penser, 32 à, 33 d et 34 autres.

On aboutit ainsi à un chiffre homophonique. Pour chiffrer « c'est ça », on peut écrire : « 13. 29. 20. 9. 26. 32 ». Pour indiquer la page et les lignes du livre utilisé, on peut commencer par leurs numéros dans le message chiffré, ce qui donne : « 250. 12. 15. 13. 29. 20. 9. 26. 32 » si on trouve le texte utilisé pour chiffrer notre texte entre les lignes 12 et 15 de la page 250.

Les erreurs du Viêt Minh… et de leurs adversaires

Au début de la guerre d'Indochine, le Viêt Minh utilisa un chiffre de Vigenère de façon particulièrement erronée : la clef, toujours de longueur cinq, était accolée en tête du message, ce qui contrevenait lourdement au principe de Kerckhoffs.



Document vietminh montrant un message chiffré en Vigenère, avec la clef TINHA en tête.

Malgré cette faiblesse du chiffre vietnamien, le conflit cryptographique avec l'armée française, déséquilibré au temps de la reconquête en 1945, quand les meilleurs cryptologues de l'armée étaient sur place, fut plutôt équilibré de ce point de vue ensuite. Les forces étaient pourtant censées disposer de machines à chiffrer de la Seconde Guerre mondiale, comme la C-36 au niveau tactique et la B-211 au niveau stratégique (voir le chapitre 11) qui auraient dû être indécryptables par le Viêt Minh. Cependant, d'après les archives vietnamiennes, bien des messages français étaient envoyés chiffrés par un Vigenère doté d'une clef trop courte, ou juste camouflés, voire en clair. Les techniques de camouflage, que nous avons déjà décrites (voir le chapitre 1), consistaient ici à seulement

remplacer quelques termes, comme « convoi » ou « tank » par d'autres d'apparence anodine comme « omelette » ou « œufs brouillés ». Cette méthode n'a guère d'espoir de permettre de garder le secret d'un grand nombre de messages. L'ennemi aura vite compris ce que recouvrent ces termes étranges.

Lors de la guerre du Vietnam qui suivit la défaite française, les Américains ne firent guère mieux et en vinrent aussi à des méthodes de camouflage, persuadés que le Viêt Cong ne serait jamais capable de comprendre leur jargon en temps réel. La NSA (National Security Agency) avait pourtant conçu Nestor, un système chiffrant la voix de bonne qualité… mais qui avait au moins deux défauts (p. suivante) : son élément (KY-38) réservé à l'infanterie était lourd (24,5 kg), même s'il y avait un net progrès par rapport au système Sigsaly de la Seconde Guerre mondiale (voir *Le chiffrement de la voix*, p. 327). De plus, Nestor ne supportait pas la chaleur humide des forêts tropicales du Sud Viêt Nam. De nombreuses unités préféraient emporter davantage de munitions plutôt que cet engin peu fiable et lourd. Cela explique l'absence de chiffrement sérieux et l'équilibre des forces entre le petit Viêt Cong et le géant américain dans la bataille des ondes.

Soldat américain portant une machine KY-38, partie « portable » du système Nestor, qui pesait en tout une bonne vingtaine de kilos.

Ce Qu'il Faut Décrypter

Un message du Viêt Minh

Le message suivant, écrit en français, est censé venir du Viêt Minh en 1954 :

TINHA TKULM BVRYM NVVAI HVFKE VMAAC BVDZU KLVLN UQRUP ACFPG GMRNI TX

Saurez-vous le décrypter ?

La méthode de Kerckhoffs

On présente souvent Auguste Kerckhoffs comme un pur théoricien, sans compétence pratique particulière. Cette idée est fausse, car il est à l'origine d'une méthode simple et lumineuse pour décrypter des messages codés avec un

chiffre poly-alphabétique. La technique est valide si l'on dispose de plusieurs messages chiffrés avec la même clef, une situation courante dans un contexte militaire. Elle consiste à écrire les messages les uns en dessous des autres, en espaçant les lettres de manière identique. En guise d'exemple, imaginons que nous interceptions les dix messages suivants :

GSJQM SIIII SHUGV JBWQV YAVPE WR
FHKCU ZSRWG JBKTI FAZFM YFVPX J
KFFPX HOCOI YFFLW NSDGH NJZUM TB
ISDCR ISSCV WOXGH FFKKP QSIKI AVUPN UEGWI IGQRY
JBMQC JFDWR NHZQR XRLTK JBTQT WSDKI WSUKZ NGZQR
XISOI WUVRE WZVPS RPIGF JQFKR WSEHS WHUWV FBU
WSGNM SSTGW XOZTI XIIUI HCEFI QWXPI RSECV I
QCLTH JGGGV YSJFI ROEFI WSEHS WHUWZ FZ
JBMQC JFIGR KCIVW IIIII SQVOI SOIF

HCKGG JBKXM SUKRV NQVFE XGRWX

La première colonne correspond à « GFKIJXWQJH ». La lettre prédominante est J, ce qui correspond à la clef possible F, puisque E serait chiffré en J (car E + F = J, comme 4 + 5 = 9). La deuxième colonne donne la clef possible O. La troisième colonne ne permet pas de conclure, la quatrième laisse penser que M est la clef possible et la quatrième ne permet pas de conclure. Les sixièmes et septièmes colonnes donnent à nouveau F et O. Cette coïncidence amène à penser que la clef est de longueur 5. Les colonnes permettant de faire une hypothèse sérieuse sur la clef sont les colonnes 8 et 9 (E et C), 14 et 15 (C et E), 18, 19 et 20 (E, B et E), 23 et 25 (R et E).

Sous l'hypothèse que la clef est de longueur 5, il reste quatre clefs possibles : « FOECE », « FORCE », « FOEBE » et « FORBE ». Seule la clef « FORCE » donne des textes valides. Voici le premier d'entre eux : « Besoin urgent de renfort. Ménard ».

La longueur de la clef pour décrypter

La méthode de Kerckhoffs demande ainsi l'interception d'un grand nombre de messages chiffrés avec la même clef. Mais, comme nous l'avons vu avec l'exemple de Jules Verne, on peut aussi décrypter un message unique chiffré par Vigenère sans en connaître la clef. En fait, l'important est d'en connaître la longueur. Montrons-le sur un cas concret. Imaginons que nous ayons intercepté le message :

LZGTV GTZHN UXLRW IIXCK BOELU GKEDX EJMDV KEWHU CXRCX SWKAE VAZLE EWIIX CKBOE WUJND VLTVG LVLCF NPRGT UXPRK IJEAG KEDBE IXAIF EVLUZ ORREA UXUOB EDXEE XCYXL FGEKT SJNRV KAVGO LMRVE ATHUM XRKNR VWUWE AEVDV LAIFE VL

Essayons de le décrypter en supposant qu'il ait été chiffré avec une clef de Vigenère de longueur trois. Si c'est bien le cas, en prenant la première lettre puis la quatrième, puis la septième et ainsi de suite en ne gardant qu'une lettre sur

trois, nous obtenons un texte chiffré par un décalage de César. Ce texte est :

LTTNL ICOUE EDEUR SAAEI COUDT LCPTP IAEEA EURAU EECLE SRAOR AURRU ADAE

Dans ce texte, la lettre la plus courante est E. Elle a la fréquence usuelle de 18 %. Sous notre hypothèse, aucun décalage n'a été opéré, de sorte que la première lettre de la clef serait A. Si nous considérons les lettres qui suivent, c'est-à-dire la deuxième, puis la cinquième, etc., nous obtenons le texte :

ZVZUR IKEGD JVWCC WEZEI KEJVV VFRUR JGDII VZRUO DEYFK JVVLV TMKVW EVIV

La lettre la plus fréquente (20 %) est maintenant V, la deuxième lettre de la clef est donc R. La dernière portion de texte est :

GGHXW XBLKX MKHXX KVLWX BWNLG LNGXK EKBXF LOEXB XXXGT NKGME HXNWE VLFL

La lettre la plus fréquente est maintenant X, la dernière lettre de la clef est donc T. Nous obtenons en définitive la clef « ART », ce qui permet de décrypter le message. Nous avons reproduit à l'occasion un message transmis le 5 septembre 1914, avec le chiffre Übchi, par le général en chef du front Ouest von Moltke aux généraux des deux armées de flanc droit, von Kluck et von Bülow :

L'intention de la Direction suprême est de refouler les Français en direction du Sud-Est en les coupant de Paris. La première armée suivra la deuxième en échelons et assurera en outre la couverture du flanc des armées.

Nous voyons donc que, pour décrypter un message chiffré en Vigenère, il suffit de connaître la longueur de la clef. Si celle-ci est courte, quelques essais suffisent pour la trouver.

Ce Qu'il Faut Décrypter

Un message en Vigenère

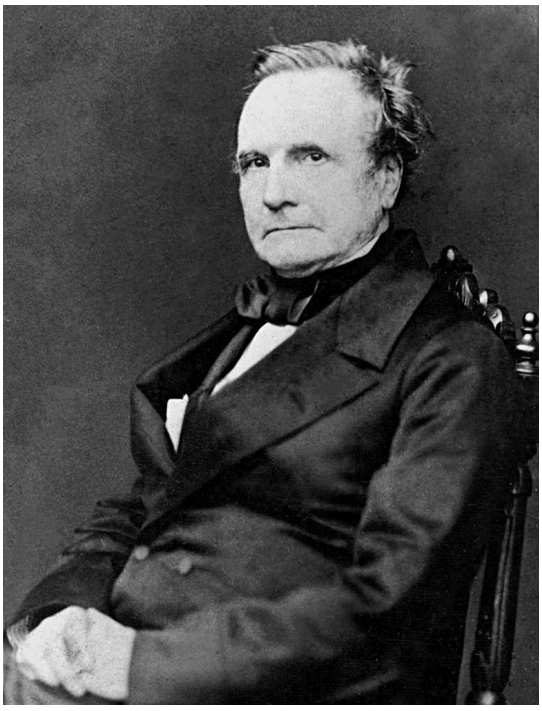
Le message suivant a été chiffré en Vigenère avec une clef de longueur cinq :

LAVES PCMRZ QTZVQ CJMJX GQCVH GPCZW JIMIP GSZLW UEAJS PTBFY USWLQ KSMKU WETVX CUAVW VRMWI TMMRY VOCIH GLIGP WSOIE PDMGE TTQVH GLIIQ GEZLW UETVB KIQCI ZVMKP GXDZM KCWIT UDIIQ GEAFR VDMKV WIBJP GSXZI EEAUE TTQCP GRQVW QNBIE USMDF NEMJH CNACI UFWII VSTVF WTQEH GGCVV TEVRT CSMEG QRMVX GCWDT VAJZP KSMDE KSQCI UTMOX TAWIH KNIZV GMMEX KMXFV VAVKE WXICI PTWLV ULMZI VLMMM EOZGW QNBVK CLMDI PTAFY HFMIX VEZIM DLMDI PTQCW UEAFR VMQJT TEKZT KTIDQ GNBVR TEBIE KTMMI TSUCE YAMKQ ASHPR KEK

Que signifie-t-il ?

Charles Babbage

Inventeur et précurseur de l'informatique avec ses machines à calculer à engrenages, l'Anglais Charles Babbage était un homme étonnant, qui avait au moins un point commun avec Bazeries : il s'amusait à lire les correspondances personnelles dans les journaux. Celles publiées au milieu du XIXe siècle dans le *Times* étaient comparables, dans leur mode de chiffrement, à celles du *Figaro* de 1890 : des chiffres de César, des atbash et des substitutions alphabétiques simples. « Le décryptement est l'un des arts les plus fascinants, et je crains d'y avoir dépensé plus de temps qu'il ne le mérite », écrivait Babbage dans son autobiographie.



Charles Babbage (1791-1871).

En 1854, Babbage intervint comme expert pour évaluer un chiffre dont l'auteur était un dentiste nommé John Thwaites. Babbage reconnut vite que le dentiste avait réinventé le chiffre de Vigenère. Il le nota dans son rapport en ajoutant que ce chiffre était facile à décrypter. Thwaites le mit au défi de décrypter un texte chiffré par sa méthode, ce que Babbage fit aisément. Comment ? En trouvant la longueur de la clef sans faire de multiples calculs de fréquences sur des sous-messages. Charles Babbage eut en fait l'idée d'attaquer cette question en cherchant des répétitions dans le message chiffré.

Ce Qu'il Faut Décrypter

Le défi du neveu de Babbage

Le neveu de Charles Babbage, Henry Hollier, mit au défi son oncle de décrypter un message dont nous vous proposons une version française légèrement simplifiée :

UVQV FFGEW

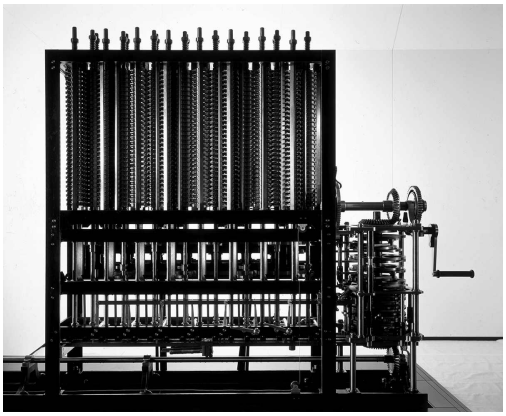
FUIE F ILL DXYJ SMLW O DIRDMLWF CYV UI JMS HSLK GHEDDIEWD ISFREZLIFWBF. GFEQX NCGW JSZXR QAQDWRM XOUVV, AP LWFM ELKWB XOOMCW HX VSOVPHXXJ QQPR. TY GMQT EYUTH NYTE KZOA JTCU CR EPNQX EFTHPT AICV KZNZI RPLDIAWY.

DSICY VIKPO IJUPWBYTFR.

PICCS
Que signifie-t-il ?

La méthode de Kasiski

Un officier prussien, Friedrich Kasiski (1805-1881), retrouva la méthode de Babbage et la publia. Injustement, elle porte depuis son nom. Les erreurs de paternité sont légion en histoire des sciences (vous vous souvenez des chiffres de César et de Vigenère ?), au point qu'on peut être tenté d'en inférer une loi générale : « Une découverte scientifique ne porte jamais le nom de son auteur. » Comme ce principe s'applique à lui-même, il est attribué à Stephen Stigler, mais a été énoncé par plusieurs autres. Dans le cas de Babbage, cet argument est renforcé par un autre plus sérieux : le gouvernement britannique n'avait aucun intérêt à divulguer qu'il pouvait décrypter un chiffre réputé inviolable à l'époque. La question était d'autant plus sensible que la Grande-Bretagne croisait le fer avec la Russie lors de la guerre de Crimée (1853-1856).



La machine de Babbage fut le premier outil que l'on puisse qualifier d'ordinateur. Babbage en énonça le principe, en fit les plans, et commença à la construire mais sans l'achever. Elle ne fut fabriquée (suivant ses plans) qu'en 1991 et fonctionna. Il est intéressant de remarquer que la naissance de

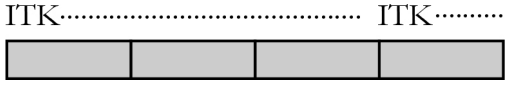
l'ordinateur pendant la Seconde Guerre mondiale est également liée au besoin en calcul de la cryptographie.

Pour fonctionner, la méthode de Kasiski nécessite des textes assez longs, et consiste à y chercher des répétitions. Voyons comment on peut l'appliquer sur le message suivant :

CV**XI**A UWQKU ZMEIO **ITK**TJ YWPFB RGTCP VJUME JVNCI WRBVZ ZJYWK NVFRV N**XI**ZF **ITK**JX ZHLFX BAIOC SBIME RRGZR NHMHX UZWEJ YMSKC GPJVA KGOFI YIKRA DAVGP WTRAF GXZDW VABNY JZKPV AOFUL VDWLM VBSSM PYEHV RLFDD PHYWA MLZFV VOBRT LZTPY RAGKR NFFKV DVYVM WITRA FGXZP RWYCF OVPCW TRAFG XZDUB VARZI JFZLA BPUUZ DTHET RIYDQ JYRLR IVNLV SNURZ YJOIK RASXV LFIUP MFVVM **XI**AQM PUEXW YYR

Dans ce message, nous avons souligné les répétitions de « XI » et « ITK ». Elles vont nous permettre de le décrypter.

Nous savons que ce message a été chiffré par la méthode de Vigenère, mais avec une clef qui nous est inconnue. Nous y trouvons plusieurs répétitions : « XI » et « ME » trois fois, « IO » deux fois et « ITK » deux fois (« XI » et « ITK » sont soulignés page précédente). Bien entendu, il peut s'agir de coïncidences, mais, plus probablement, le même texte a été chiffré avec la même partie de la clef. Examinons le cas le plus long, celui de « ITK ». S'il s'agit bien des mêmes trois lettres chiffrées avec la même partie de la clef, nous retrouvons plusieurs fois cette clef répétée entre le I de la première occurrence et celui de la deuxième. Dans ce cas, la longueur de la clef divise la distance entre ces deux I, soit 45.



Si ITK représente deux parties identiques du message, chiffrées avec la même partie de la clef, la clef a été répétée plusieurs fois entre ces occurrences (pavés en gris sur la figure).

Nous pouvons reprendre le raisonnement pour les répétitions de « XI ». Elles sont séparées de 54, puis de 234 lettres. Avec l'hypothèse précédente, nous obtenons une longueur de clef divisant 54 et 234. Le plus grand diviseur commun de ces trois nombres (45, 54 et 234) est 9. Il est donc logique de vérifier si la clef est bien de longueur 9. Pour cela, divisons le message en neuf parties, en partant d'une des neuf premières lettres, puis en décalant de 9 à chaque fois. Si notre supposition est bonne, chaque partie a été chiffrée par simple décalage. Le premier neuvième du texte est :

CUTTV ZVJIR UCFVX JLSFL LRVXV XIUYV YVVE

La lettre la plus fréquente est V (plus de 23 %) : elle représente E. La première lettre de la clef est donc R. Nous faisons de même pour les huit autres groupes :

VZJCN JNXOG ZGIGZ ZVMDZ ZNMZP ZJZDN JLMX
XMYPC YXZCZ WPYPD KDPDF TFWPC DFDQL OFXW
IEWVW WIHSR EJIWW PWYPV PFIRW UZTJV IIIY
AIPJW KZLBN JVKTV VLEHV YKTWT BLHYS KUAY
UOFUR NFFIH YARRA AMHYO RVRYR VAERN RPQR
WIBMB VIXMM MKAAB OVVWB ADACA ABTLU AMM
QTREV FTBEH SGDFN FBRAR GVFFF RPRRR SFP
KKGJZ RKARX KOAGY USLMT KYGOG ZUIIZ XVU

Dans cinq cas, une lettre est majoritaire. Dans les autres, plusieurs le sont. Nous obtenons la clef « RVL*xy*N*zw*G » où *x* est E ou S, *y* R, G ou H, *z* W ou I et *w* B ou N. *A priori*, 24 clefs sont possibles en faisant varier les possibilités des inconnues *x*, *y*, *z* et *w*. Plutôt que de les essayer toutes, nous utilisons les lettres déjà trouvées sur le début du message : « **LAM**IA **H**WQ**ED** » où nous avons souligné les lettres décryptées. Avant le H (sixième lettre), nous avons probablement un P ou un T. Les trois possibilités de clefs R, G ou H donnent H, U ou T, donc c'est T. La quatrième lettre est donc un E, ce qui donne la clef E. À ce stade, la clef est « RVLEHN*zw*G ». Nous obtenons :

LAMET HWQ**ED EBABB** IT**ECO NSIS**B R**ACHE RCH**ME **DESRE PE**BV**T IONSDA**

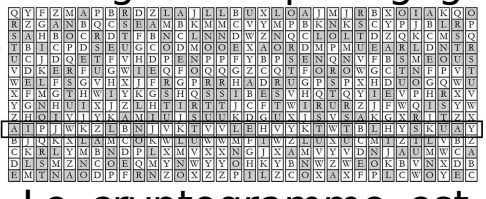
Après le H, la lettre W a été chiffrée en W ou I, il s'agit donc de A ou de O. La lettre Q a été chiffrée en B ou N, il s'agit de O ou D. Les seuls choix à faire sens sont O et D dans l'ordre, ce qui donne « la méthode ». La clef est donc « RVLEHNING » et le message :

> La méthode de Babbage consiste à chercher des répétitions pour trouver la longueur de la clef. Elle fonctionne dès que les messages sont assez longs, ou assez nombreux. Une fois la longueur obtenue, il reste à subdiviser le message en plusieurs messages, qui se trouvent chiffrés par le chiffre de César. La méthode des fréquences permet de conclure

Bien entendu, la méthode de Kasiski est utile pour décrypter tout chiffre poly-alphabétique, en particulier celui de Beaufort.

La méthode de saint Urlo

Une idée similaire, mais qui fonctionne de façon plus générale, consiste à se munir de bandes de papier où sont inscrites à espaces réguliers toutes les lettres de l'alphabet, et où la lettre E et celles composant l'expression « saint Urlo » ont été grisées. Pourquoi les griser ? Tout simplement parce que dans un texte non chiffré, elles représentent 80 % des lettres utilisées, comme nous l'indiquions au chapitre 3. Ce texte apparaîtra donc en gris. On place les bandes verticalement les unes à côté des autres, de façon à former sur une ligne le cryptogramme cherché, ici « AIPJW KZLBN JVKTV VLEHV YKTWT BLHYS KUAY » (nous avons repris la cinquième phrase de l'exemple précédent, celle qui nous a posé le plus de problèmes). En réduisant le tableau au rectangle utile pour gagner en encombrement, on obtient :



Le cryptogramme est fléché et entouré, la ligne la plus grisée est juste fléchée. C'est probablement celle du clair,

puisqu'un grand nombre de ses lettres font partie des lettres « E saint Urlo », représentant 80 % des lettres dans un texte clair. Puisque A est changé en T, la clef est H, ce qu'on avait déjà trouvé. Bien entendu, on peut facilement informatiser la question. Chaque ligne a un score « saint Urlo » en comptant les apparitions de E et de saint Urlo sur cette ligne. Il suffit de considérer le meilleur score : il correspond très probablement à la clef. Sinon, on passe aux scores suivants, la clef est sans aucun doute parmi eux.

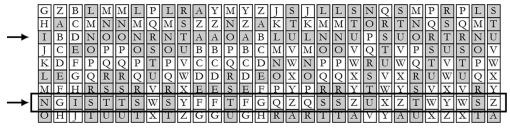
La méthode de saint Urlo a l'avantage de ne pas être sensible à la présence ou non de E dans le texte clair, comme l'illustre l'exemple suivant :

NTNGI AIWAS IFTVE TUNSA HWABS TVYQY FTYFI FTVYF DNGWV QUBZQ YQIHS ONSBD ZQYUI FXIFZ ZFTVS WWAYA HWABS KBZ

Remarquons que « NG » est répété à la distance de 39 et « WABS » à la distance de 60 : la clef est donc probablement de longueur 3, diviseur commun de 39 et de 60. Cela nous mène à considérer les trois mots :

NGIST TSWSY FFTFG QZQSS ZUXZT WYWSZ
TIWIV UAATQ TIVDW UQIOB QIIZV WAAK
NAAFE NHBVY YFYNV BYHND YFFFS AHBB

La méthode de saint Urlo appliquée au premier mot donne :



De même que précédemment, la ligne du clair apparaît plus grisée que les autres, ainsi I est chiffré en N. La première lettre de la clef est donc F. On recommence avec les deux autres mots, on obtient finalement la clef « FIN » et le texte :

Il abandonna son roman sur son lit. Il alla à son lavabo ; il mouilla un gant qu'il passa sur son front, sur son cou.

Il s’agit d’un court extrait de *La Disparition*, le roman que Georges Perec écrivit sans la lettre E. Une carence qui n’empêche pas le décryptement, contrairement à ce qu’on pourrait penser.

Le mot probable de Bazeries

Comme les héros de Jules Verne l'ont montré, la méthode du mot probable est précieuse pour décrypter un message chiffré en Vigenère. C'est Étienne Bazeries qui a le premier conçu comment s'y prendre. Reprenons le message de von Moltke :

LZGTV GTZHN UXLRW IIXCK BOELU GKEDX EJMDV KEWHU CXRCX SWKAE VAZLE EWIIX CKBOE WUJND VLTVG LVLCF NPRGT UXPRK IJEAG KEDBE IXAIF EVLUZ ORREA UXUOB EDXEE XCYXL FGEKT SJNRV KAVGO LMRVE ATHUM XRKNR VWUWE AEVDV LAIFE VL

Cherchons-y le mot « direction ». Si ces neuf lettres s'y trouvent, additionnées de la clef éventuellement répétée ou d'une partie simplement, elles donnent neuf lettres du message chiffré. Imaginons qu'il s'agisse des neuf premières lettres. En ajoutant le mot « DIRECTION » au mot qui l'a chiffré, nous obtenons « LZGTVGTZH » donc en retranchant « DIRECTION » à « LZGTVGTZH », nous obtenons le mot qui l'a chiffré.

L	Z	G	T	V	G	T	Z	H
D	I	R	E	C	T	I	O	N
3	8	17	5	2	19	8	14	13
I	R	P	P	T	N	L	L	U

On retranche DIRECTION aux neuf premiers caractères. Le résultat n'a aucun sens. Cette clef ne respecte pas les habitudes de l'époque, qui voulaient qu'elles soient faciles à retenir.

Le mot obtenu, « IRPPTNLLU », ne correspond pas aux clefs normalement en usage. Recommençons avec les mots de neuf lettres suivants : « ZGTVGTZHN », « GTVGTZHNU », etc. Arrivés à « WIIXCKBOE », nous obtenons « TARTARTAR ».

Il suffit alors de tâtonner un peu pour reconstituer la clef « ART ».

Cette méthode montre une faiblesse supplémentaire du chiffre de Vigenère : les clefs ont un sens pour être retenues par cœur… ce qui permet de les reconnaître. De plus, on voit que les clefs courtes se prêtent plus facilement au décryptement.

Ce Qu'il Faut Décrypter

Un message en Beaufort

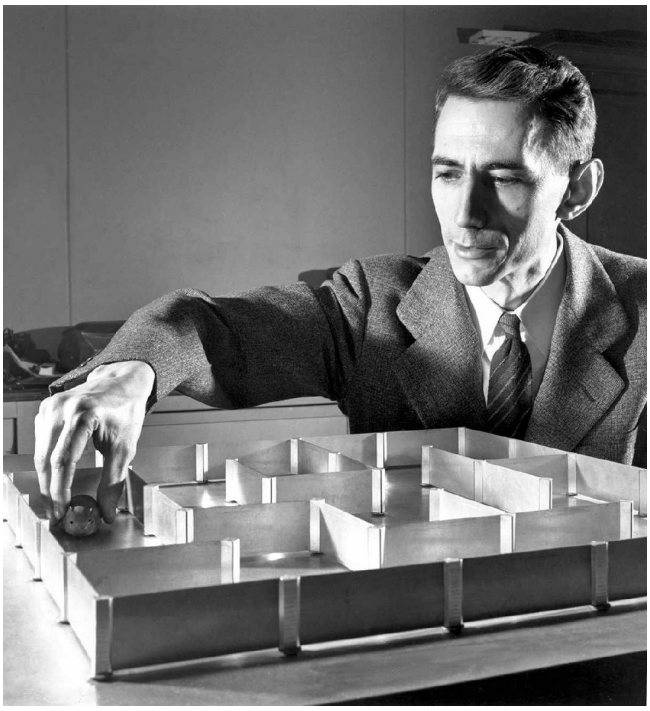
Le message suivant a été chiffré en Beaufort :

BWRIV DLHIO PJYWP VWGRW FYJMO JYYYN KHMOJ PYNNI VFYJP CPFYV DLYNM GRJJN

Que signifie-t-il ?

Le masque jetable

Pour éviter le décryptement par la méthode de Kasiski (qui consiste à rechercher des répétitions dans la version chiffrée), le cryptologue américain Gilbert Vernam (1890-1960) eut l'idée d'utiliser des clefs aussi longues que les messages. Joseph Mauborgne, déjà rencontré à propos du chiffre de Playfair, estima qu'il valait mieux que cette clef soit aléatoire. Plus tard, en créant la théorie de l'information, Claude Shannon (1916-2001) démontra que ce chiffre est alors inviolable. La raison est simple : en chiffrant un texte avec une clef aléatoire, le texte lui-même devient aléatoire. En revanche, la même clef ne doit pas être utilisée deux fois. Il faut la jeter après une seule utilisation, d'où son nom de masque jetable (*one time pad* en anglais, souvent traduit en « clef une fois »). Pourquoi jeter la clef après un seul usage ? La raison est qu'en soustrayant deux messages chiffrés avec la même clef, on la fait disparaître et le chiffre devient cassable par la méthode du mot probable.



Père de la théorie de l'information, Claude Shannon a montré que, correctement appliqué, le masque jetable est inviolable. C'est aussi un précurseur de l'intelligence artificielle. Ici il est photographié avec l'une de ses inventions : une souris mécanique trouvant seule son chemin dans un labyrinthe.

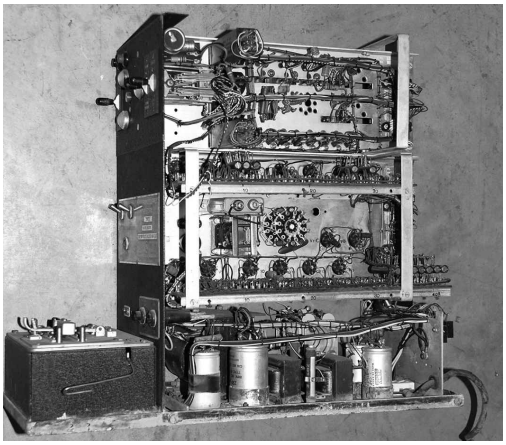
D'après les archives britanniques, les Soviétiques firent cette erreur par mesure d'économie dans les années 1930. Ils persistèrent dans leur erreur, ce qui facilita le projet *Venona* américain de décryptement des messages des services de renseignements soviétiques. Trois mille messages furent ainsi décryptés totalement ou partiellement. Une des conséquences a été la détection d'espions soviétiques comme les époux Rosenberg et les « cinq de Cambridge », dont le célèbre agent double Kim Philby.

Cette faiblesse du masque jetable, pourtant mathématiquement indécryptable, rappelle en même temps la différence entre la théorie et la pratique et surtout qu'un théorème de mathématiques a des hypothèses strictes – ici le côté aléatoire des clefs et leur utilisation unique. On ne

peut l'invoquer en dehors de ses conditions d'application, même si l'idée est tentante pour qui ne maîtrise pas ces questions.

Les autres faiblesses de ce chiffre « parfait » sont la taille, la création et la transmission des clefs. Nous reviendrons sur ces points car il n'est pas aisé de créer de l'aléatoire. Hors du milieu des mathématiques, le mot « aléatoire » est souvent mal interprété et les gens ont souvent l'impression qu'on peut se contenter de créer une liste de nombres qui viennent spontanément à l'esprit… Or ceux-ci sont rarement vraiment aléatoires ! Aujourd'hui, le masque jetable est surtout utilisé à des niveaux demandant un secret élevé, comme la diplomatie. Par exemple, il a été au cœur du « téléphone rouge » reliant Washington et Moscou.

Le téléphone rouge



Cœur du « téléphone rouge » d'origine. La clef est inscrite sur une bande de papier perforé, qui est lue grâce au lecteur à gauche de la photo (la petite boîte). Le gros appareil de droite effectue le chiffrement.

Le téléphone rouge désignait une ligne de communication directe établie entre la Maison-Blanche et le Kremlin par John Kennedy et Nikita Khrouchtchev, après que la crise des

missiles de Cuba avait mené le monde au bord de la guerre en 1962. Il s'agit d'une métaphore reprise et popularisée par les médias, la ligne étant en réalité un fax. Elle a permis de désamorcer par la suite nombre de situations conflictuelles entre le bloc communiste et le monde occidental.

La ligne était chiffrée grâce au principe du masque jetable sur des messages en binaire (suite de 0 et de 1). Chaque pays fournissait la sienne, la clef finale étant la somme (sans retenue) des deux. Ainsi, il était impossible à l'un des deux partenaires de tricher en fournissant une clef semblant aléatoire mais ne l'étant pas, ou plutôt cela n'aurait servi à rien. L'utilisation de la méthode avait de plus l'avantage de ne livrer aucun secret à l'adversaire. Les clefs de chaque pays étaient transportées par valise diplomatique et détruites après chaque utilisation. Nous reviendrons sur la question, puisqu'elle ouvre l'ère numérique.

Le chiffre du Che

Après son succès comme compagnon de Fidel Castro dans la guérilla cubaine, Ernesto Guevara, dit le Che, tenta d'exporter la révolution en Bolivie. Le 8 octobre 1967, il fut capturé par l'armée de ce pays, et exécuté le lendemain même. On trouva sur lui une description du chiffre qu'il utilisait pour transmettre ses messages à Fidel Castro. Il commence par une substitution alphabétique simple en nombres d'un ou deux chiffres.

A	B	C	D	E	F	G	H	I	J	K	L	M
6	38	32	4	8	30	36	34	39	31	78	72	70

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
76	9	79	71	58	2	0	52	50	56	54	1	59

Première étape du chiffrement de Che Guevara.

Les chiffres sont ensuite groupés par cinq, puis additionnés à une suite de chiffres aléatoires partagée par Fidel Castro et Ernesto Guevara. Cette addition se fait sans retenue, ainsi : 24567 + 78351 = 92818. Il s'agit donc d'une clef de Vernam (autrement dit, de longueur égale à celle du message).

Ernesto Guevara utilisait une clef de Vernam, comme le montre ce brouillon, trouvé sur lui à sa mort.

Ce type de chiffre a été pratiqué par des espions soviétiques, dont Georges Beaufils (1913-2002), cet ancien FTP suspecté d’avoir été recruté par le GRU, les renseignements militaires. Un livre de nombres aléatoires et des feuilles contenant des soustractions sans retenues, trouvés dans ses affaires, servirent de pièces à conviction lors de son procès. Il fut condamné à huit ans de prison en 1978.

Les stations de nombres

Il est tentant de lier ces listes interminables de chiffres copiées par Che Guevera et Georges Beaufils à des émissions étranges qu'on peut entendre sur les ondes courtes. On les nomme stations de nombres car, mis à part un indicatif ressemblant à ceux des radios ordinaires, elles ne diffusent que des nombres dits par une voix artificielle (c'est-à-dire créée par une machine et non un être humain), de longues litanies peu romantiques comme : « trois neuf zéro un cinq » suivi d'un espace, éventuellement une ou plusieurs répétitions (pour s'assurer de la bonne compréhension de l'auditeur), puis d'autres nombres. Le tout forme visiblement un message qu'on ne peut décrypter qu'en connaissant la méthode et la clef utilisées.

Ce type de stations a commencé à émettre en morse vers la fin de la Première Guerre mondiale, mais leurs heures de gloire furent au temps de la guerre froide. Plusieurs réseaux d'espionnage semblent avoir profité de ces stations pour communiquer. Elles ont presque disparu à la chute du mur de Berlin. J'écris « presque » car une poignée de ces stations demeurent. À l'heure d'Internet, on peut légitimement se demander pourquoi. Peut-être pour ne pas perdre la capacité d'échanger en cas de coupure du réseau ?

Les coïncidences de Friedman

Revenons aux substitutions poly-alphabétiques. Pour déterminer la longueur d'une clef de Vigenère, le cryptologue de l'armée américaine William Friedman eut l'idée d'introduire un indice invariable par permutation des lettres. Ainsi, sa valeur n'était pas affectée par une

substitution alphabétique simple, telles celles engendrées par le chiffre de César. L'intérêt de cet indice est qu'une fois calculé pour le message chiffré, on pourra déduire directement la longueur de la clef, ce qui facilitera le décryptement.

William Friedman (1891-1969), cryptologue de l'armée américaine puis cryptologue en chef de la NSA après la Seconde Guerre mondiale.

Pour obtenir un tel indice, l'idée la plus simple est d'additionner les carrés des fréquences des lettres. Plus précisément, dans un texte T donné, on compte le nombre d'occurrences de chaque lettre : n_A pour A, n_B pour B,…, n_Z pour Z. On en fait la somme n, qui est donc la longueur du texte, puis la somme des carrés n_A^2, n_B^2,…, n_Z^2. On divise enfin cette dernière somme par le carré de n. Si on échange les lettres, les positions des carrés des fréquences sont modifiées dans la somme, mais celle-ci reste identique puisque tous les carrés s'y retrouvent malgré la

permutation. Ce nombre n'ayant pas de sens concret, on lui préfère un autre, très proche, appelé indice de coïncidence.

Indice de coïncidence

L'indice de coïncidence d'un texte T est la probabilité que deux lettres tirées au hasard dans ce texte coïncident. Notons S la somme des carrés des fréquences des lettres et I_C l'indice de coïncidence. On démontre que les deux notions sont liées par la formule : $(n-1)\,I_C = n\,S - 1$.

Si le texte est relativement long, n et $n-1$ sont à peu près égaux et 1 est négligeable devant n. Ainsi, S et I_C peuvent être confondus, ce que nous ferons par la suite.

Sans moyen électronique, le calcul est relativement long. Effectuons-le sur un texte court pour en montrer la difficulté. Soit donc le texte : « calcul de l'indice de coïncidence de Friedman ». Nous calculons les nombres d'occurrences de chaque lettre, leurs carrés, puis nous faisons les sommes des deux.

lettres	A	C	D	E	F	I	L	M	N	O	R	U	total
nombre	2	6	6	7	1	5	3	1	4	1	1	1	38
carré	4	36	36	49	1	25	9	1	16	1	1	1	180

Calcul de l'indice de coïncidence.

La somme des fréquences au carré est donc égale à 180 divisé par 38 au carré, soit : 0,12. Il faut retrancher 1/37 pour obtenir l'indice de coïncidence. Il est donc égal à 0,10.

À partir des fréquences usuelles, il est possible de déterminer l'indice de coïncidence moyen d'un texte en français, ou dans d'autres langues, éventuellement codé par un chiffre tel celui de César. Il suffit de faire la somme des fréquences moyennes au carré.

A	B	C	D	E	F	G	H	I	J	K	L	M
8,4	1,1	3,0	4,2	17,3	1,1	1,3	0,9	7,3	0,3	0,1	6,0	3,0
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
7,1	5,3	3,0	1,0	6,5	8,1	7,1	5,7	1,3	0,1	0,4	0,3	0,1

Tableau de fréquences des lettres en français, exprimées en pourcentage.

En français, l'indice de coïncidence moyen est donc la somme :

$0{,}084^2 + 0{,}011^2 + \ldots + 0{,}001^2 = 0{,}0746$.

Dans le cas d'un message où les lettres seraient choisies au hasard, nous obtenons une fréquence moyenne de 1/26. L'indice est donc égal à 26 fois $(1/26)^2$, c'est-à-dire à 1/26, soit 0,038. Il s'agit de l'indice de coïncidence moyen d'un texte aléatoire.

Reprenons le message chiffré précédent (« CVXIA… PUEXW YYR ») fort de cette nouvelle arme. Son indice de coïncidence est égal à 0,042, plus proche de celui d'un texte aléatoire que celui d'un texte moyen. Il n'est donc pas chiffré via une substitution mono-alphabétique, la clef n'est pas de longueur 1. Considérons alors les textes obtenus en partant de la première lettre et en ne gardant qu'une lettre sur deux, sur trois, etc. Nous obtenons des indices de coïncidences compris entre celui d'un texte aléatoire et celui d'un texte moyen.

clef	1	2	3	4	5	6	7	8	9

indice	0,04	0,04	0,06	0,05	0,04	0,06	0,04	0,03	0,08

Indices de coïncidences.

Arrivés à 9, nous obtenons un indice proche de l'indice moyen. Nous retrouvons par un simple calcul que la longueur de la clef est égale à 9. La suite est identique à ce qui précède et reste automatisable.

Ce Qu'il Faut Décrypter

Un autre message en Vigenère

Le message suivant a été chiffré en Vigenère :

CVLLG SAIVH NZOEL LNRIV GAXVS LUHMJ OIMLX VPZKV ALEJY HCKEJ WBHKR FGJWI ELLLU LFVNL NRLRA HWYEG HPHKU VLLNC EXXYY JDVEH PRNKE VOIDVL LNRRI HUXZE JWLFR RIBLL VPFNC UETGH YNVRU XBHRD FNGYI ADXBL JEKIY YEDIX QOJQL TALFI JHBKL AKKLN FNEXH OODVF HLTHR GKCJE JWLMV GRKPN VAJZY IJSZX YYDEE MJIES KKBCK EJEHL XEDXU NWATH UHVEJ KLWFU MXYNV SVGWU ITZXK UESCX BLDIC BLOUU EMVCK DVYLO ZLCTN YHUZEH CJSVE PVIEV GHVFR UNUYT OLKZC MEJNY FRQLX SFVSV ISUTE EMSYJ PRZHS VUILK YJJRG NUUAJ LVLKE UXYUU ERNEC EFFKT YJATM PIENV LWUIU EXCIZ LVMYC RNXNS UZRVX AMLPG HYNRN KEHWR BRGLX VPRBS FZSHN PMVRK WLGRI JHUZC OKMHH KEREP HUIVG LNRSR YHGZL CX

Saurez-vous le décrypter ?

Ce long parcours sur les substitutions poly-alphabétiques, commencé à la Renaissance et semblant se terminer avec le masque jetable et le téléphone rouge, va se poursuivre avec les machines à chiffrer, dont la plus célèbre est Enigma. Avant cela, les insuffisances de la méthode poussèrent les cryptologues à marier les deux grandes méthodes de chiffrement, substitution et transposition, ce qui ouvre la voie au surchiffrement, comme nous allons le découvrir.

9
Le coffre-fort à code secret : le surchiffrement

Vous souvenez-vous du premier chapitre et du « miracle de la Vistule » ? En 1920, pris en tenaille par les forces russes, les Polonais étaient parvenus à décrypter les transmissions ennemies et à renverser l'issue du conflit ; vraisemblablement les Russes employaient alors un code par substitution. Et la bataille de la Marne, perdue par les Allemands en 1914 ? Les Français avaient réussi à décrypter le chiffre allemand qui employait, lui, une méthode à transposition. Deux défaites historiques dues à l'impact décisif des services du chiffre. Mais aussi et surtout, deux échecs patents des techniques de substitution et de transposition.

Ni les méthodes de substitution ni celles de transposition n'étant parfaites, il est logique que les cryptologues se soient tournés vers un mélange des deux, dès la fin du XIX^e^ siècle. Voici un florilège des meilleures méthodes de « surchiffrement » qui ont permis aux armées de la fin du XIX^e^ siècle et de la Première Guerre mondiale, tous pays confondus, d'améliorer singulièrement la sécurité de leurs codes. Surchiffrer un chiffre, c'est un peu comme l'enfermer dans un coffre-fort pour en accroître la sûreté. Ce serait une surprise si je vous disais qu'aucun de ces surchiffrements n'a résisté longtemps ?

Cryptographie à l'« srevne » (à l'envers) Selon Étienne Bazeries, en 1886, le général français Boulanger, alors ministre de la Guerre, affectionnait un chiffre fondé sur un chiffre de Vigenère surchiffré par une transposition très simple, puisqu'il s'agit de l'écriture à l'envers. Avec la clef « CROIX », le message « Boulanger a fait adopter le fusil Lebel » devient d'abord :

B	O	U	L	A	N	G	E	R	A	F	A	I	T	A	D	O
C	R	O	I	X	C	R	O	I	X	C	R	O	I	X	C	R
D	F	I	T	X	P	X	S	Z	X	H	R	W	B	X	F	F
P	T	E	R	L	E	F	U	S	I	L	L	E	B	E	L	
O	I	X	C	R	O	I	X	C	R	O	I	X	C	R	O	
D	B	B	T	C	S	N	R	U	Z	Z	T	B	D	V	Z	

Soit : « DFITX PXSZX HRWBX FFDBB TCSNR UZZTB DVZ », qu'il ne reste plus qu'à écrire à l'envers, ce qui fournit le cryptogramme : « ZVDBT ZZURN SCTBB DFFXB WRHXZ SXPXT IFD ».

Ce Qu'il Faut Décrypter

Un message de Bazeries

Étienne Bazeries a choisi le chiffre de Boulanger pour créer le cryptogramme suivant :

AWAQG KQZKG STNVX MWFKH WTQRO WQCMP WAIFX WRGVJ UIQJP AWAJG DBBFU JQFMW GKSUC KMZZE ANTZF KCZGU WTGKG JKSJU WT

Saurez-vous le décrypter ?

Le chiffre de Delastelle résume mieux l'époque que celui de Boulanger. De façon étonnante, il utilise l'antique carré de Polybe. Cryptologue amateur à une époque où le décryptement était déjà devenu une affaire de militaires et d'universitaires, Félix Delastelle (1840-1902) eut l'idée de mélanger un chiffrement par substitution par carré de Polybe et une transposition. Nous commençons par remplir le carré grâce à un petit poème, par exemple avec « Le châtiment de la cuisson appliqué aux imposteurs » d'Alphonse Allais :

Chaque fois que les gens découvrent son mensonge,
Le châtiment lui vient, par la colère accrue.
« Je suis cuit, je suis cuit ! » gémit-il comme en songe.
Le menteur n'est jamais cru.

	1	2	3	4	5
1	C	H	A	Q	U
2	E	F	O	I	S
3	L	G	N	D	V
4	R	T	M	P	J
5	B	K	X	Y	Z

Carré de Polybe, première étape du chiffre de Delastelle : on remplit le carré avec le poème en supprimant les doublons et en ajoutant ensuite les lettres manquantes.

Ce poème est la première partie de la clef. La seconde est un nombre, par exemple 5, destiné à grouper les lettres. Ici, nous les assemblons donc 5 par 5. Considérons le message « Attaquez demain à quatre heures ». Pour le chiffrer, nous codons chaque lettre suivant le carré ci-dessus. Ainsi, A est codé 13 (ligne et colonne de A dans le carré), ce que nous écrivons en colonne. Nous complétons le message pour obtenir un nombre de lettres multiple de 5.

A	T	T	A	Q	U	E	Z	D	E	M	A	I	N	A
1	4	4	1	1	1	2	5	3	2	4	1	2	3	1
3	2	2	3	4	5	1	5	4	1	3	3	4	3	3
Q	U	A	T	R	E	H	E	U	R	E	S	X	X	X
1	1	1	4	4	2	1	2	1	4	2	2	5	5	5
4	5	3	2	1	1	2	1	5	1	1	5	3	3	3

Première étape du chiffrement de Delastelle.

Nous lisons alors les cinq premiers chiffres de la première ligne puis ceux de la seconde, puis les cinq suivants de la première ligne, etc. En les groupant deux par deux, cela donne :

14 41 13 22 34 12 53 25 15 41 41 23 13 34 33 11 14 44 53 21 21 21 41 21 51 22 55 51 53 33

Pour finir, nous utilisons le carré pour retraduire ces nombres en lettres et les groupons par cinq :

QRAFD HXSUR ROADN CQPXE EEREB FZBXN

Si on connaît les clefs, le déchiffrement s'effectue en sens inverse. Si on connaît le principe sans connaître les clefs, on peut attaquer séparément la substitution et la transposition (voir également *Le chiffre ADFGX* et *L'ajout du V : le chiffre ADFGVX*, p. 256 et 261). Dans tous les cas, un tel chiffre demande un changement quotidien des clefs, si on doit y recourir de manière intensive.

Une recette périgourdine

Une recette périgourdine a été chiffrée par un chiffre de Vigenère avant d'être surchiffrée par la transposition la plus simple qui soit :

FJXAI LILSQ ILHSE DOIMW FKYIG WYWXC YMREI AGNET GJQUO WKMHS ECESM KFZSX GJHVC HIAHL RQJJH ASMGV OWXZO UIQCK ITNJW QIHIZ WZGMF NENSQ ILHSE DOJXV ONFUO JVCHF VMDRI BOWIA CUIZS NSNSQ DMGXM IZQSW QQETN JVQHJ VAWFV NIFIZ IJLMB ZVMBN VIAEI AGNET QFROC HILSW VMJSY HSYYW XFVMB NVZSY IVIXR IRJPH SHETD EIZJN SXNJP IGJPH SAVMB JHMZE IOBTT MSWYM VJRCH SELBJ TTSXW WFLIL SUYWG FWMFJ PTWZG FIJHK SAECO JHQZU QMFWI QRFPI GSYAB FHZSN XVSXE ZUJMW TJPHS UQMFY

Saurez-vous exécuter cette recette ?

Le chiffre de Bazeries

Autre méthode de surchiffrement, le chiffre de Bazeries consiste en une transposition suivie d'une substitution mono-alphabétique. La clef est un nombre inférieur à un million, comme 4965. On remplit un carré de côté 5 (sans le W) avec son écriture en toutes lettres : quatre mille neuf cent soixante-cinq. Ce carré donne une substitution mono-alphabétique quand on le met en correspondance avec le carré rempli avec les lettres dans l'ordre (et écrites en colonnes) : A se transforme en Q, B en E, etc.

Q	U	A	T	R
E	M	I	L	N
F	C	S	O	X
B	D	G	H	J
K	P	V	Y	Z

A	F	K	P	U
B	G	L	Q	V
C	H	M	R	X
D	I	N	S	Y
E	J	O	T	Z

Le message à chiffrer est découpé en groupes de 4, 9, 6 et 5 lettres. Ainsi de suite en ajoutant des nulles si besoin, on écrit chaque groupe à l'envers puis on effectue la substitution donnée par le carré. Chiffrons le message : « transposer et substituer, bonne recette ».

clef	4	9	6	5	4	9
1	TRAN	SPOSERETS	UBSTIT	UERBO	NNER	ECETTEXXX
2	NART	STERESOPS	TITSBU	OBREU	RENN	XXXETTECE
3	GQOY	HYKOKHVTH	YDYHER	VEOKR	OKGG	XXXKYYKFK

Le message chiffré est donc :

GQOYH YKOKH VTHYD YHERV EOKRO KGGXX XKYYK FK

Le chiffre ABC

Quand les Allemands saisirent, en lisant *Le Matin*, que leur chiffre Übchi n'avait rien de secret pour l'armée française, ils firent le choix d'un nouveau chiffre, du type de celui de Delastelle. Plus précisément, il s'agissait d'un chiffre de Vigenère de clef « ABC », d'où son nom donné par les Français.

Cette substitution était suivie d'une simple transposition de colonnes, modifiée régulièrement au moyen d'une clef. La grosse faiblesse résidait dans la clef « ABC ». Aidés par quelques erreurs des chiffreurs allemands, les décrypteurs de l'armée française n'eurent besoin que de trois semaines pour comprendre le système. Il devint alors aisé à décrypter, d'autant plus qu'un jeune polytechnicien, Georges Painvin, sans doute le cryptologue le plus brillant de toute la guerre, trouva un moyen rapide pour découvrir la clef.

Georges Painvin (1886-1980) se révéla un décrypteur de génie durant la Grande Guerre.

Il faut avouer que l'amateurisme des Allemands dans ce domaine l'aida beaucoup. En particulier, ces derniers multipliaient les erreurs de protocole, en choisissant des clefs « patriotiques » telles « VATERLAND », « KAISER » ou « DEUTSCHLAND » et en répétant chaque matin des messages comme « Nuit calme, rien à signaler. » Des termes qui fournissaient à leurs adversaires autant de mots probables… Une astuce que les Français déployèrent fut de bombarder les tranchées ennemies et de feindre une attaque pour amener les Allemands à produire une foule de mots probables, ce que ceux-ci firent toujours avec obligeance.

Les Allemands modifièrent intelligemment leur système en 1915 en émettant de plus 50 % de messages sans véritable sens militaire. Ce qui n'empêcha pas le nouveau chiffre d'être décrypté. La clef « ABC » avait simplement été changée en « ABCD », en interrompant ce chiffrement (et en

le reprenant à A) en fonction des nombres constituant la clef de la transposition. Les Allemands retournèrent ensuite à des chiffres par substitution, mono-alphabétique ou poly-alphabétique… que les Français décryptèrent progressivement. Ils renoncèrent à ces codes fin 1916 pour revenir aux méthodes de transposition.

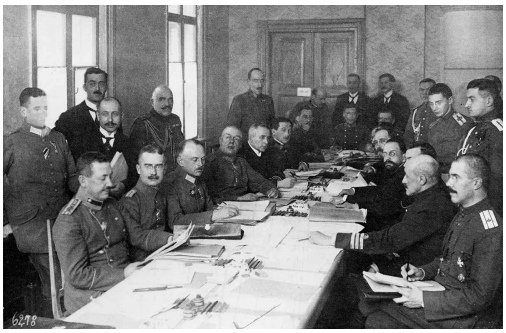
Ce Qu'il Faut Décrypter

Un message en ABC

On intercepte le message suivant, dont on sait qu'il est chiffré en ABC :
BEMVU REBFIK GEPBK VURRR LCIMU RBELS OTENH BUJBF OBJFT CGTGW GJW
Saurez-vous y voir clair ?

Le chiffre ADFGX

Le 15 décembre 1917, l'Allemagne signait l'armistice avec la Russie bolchevique. La paix à l'Est permettait aux armées allemandes de se concentrer sur le front Ouest. Une course de vitesse s'engagea alors entre Américains et Allemands, entre l'arrivée de l'armée américaine sur le front et celle des renforts allemands. Et bien sûr, pour garantir l'effet de surprise, il fallait pouvoir communiquer sans être entendu par l'adversaire. Le haut commandement allemand ayant compris que ses codes n'étaient guère secrets, il décida d'en changer avant le jour de la nouvelle offensive. Pour une fois, la question fut prise au sérieux et une conférence sur le thème fut organisée à Berlin, où les cryptologues croisèrent le fer pour savoir quel chiffre l'Allemagne devait à présent préférer. Le code inventé par un colonel au nom prédestiné de Fritz Nebel (« brouillard » en allemand) fut choisi pour mystifier les Français.



Signature de l'armistice à l'Est le 15 décembre 1917, qui faillit changer le cours de la guerre.

Même s'il était malin, le chiffre de Nebel n'offrait rien d'original par rapport à ce que savaient décrypter les services de renseignement de l'Alliance. Avant de voir la méthode que déploya Georges Painvin pour le casser, voyons comment Fritz Nebel l'avait conçu. Tout d'abord, pour éviter les confusions à la réception, le système n'utilisait que cinq lettres, toutes très éloignées en code Morse : A, D, F, G et X.

• — : A
— • • : D
• • — • : F
— — • : G
— • • — : X
• • • — : V

Les codes Morse des lettres A, D, F, G, X et V.

C'est ainsi que les décrypteurs français le nommèrent « chiffre ADFGX », tandis que les Allemands le désignaient sous le nom de *Gedefu 18*, ce qui signifie « Geheimschrift der Funker 18 », soit « chiffre des radiotélégraphistes 18 ». Il était fondé sur un carré de Polybe construit à partir d'une clef changée quotidiennement. Pour s'adapter à l'allemand, le I et le J étaient confondus et non le V et le W. Avec la clef « Geheimschrift der Funker », cela donne (comme d'habitude, les répétitions sont supprimées et les blancs comblés avec les lettres manquantes) :

	A	D	F	G	X
A	G	E	H	I	M
D	S	C	R	F	T
F	D	U	N	K	A
G	B	L	O	P	Q
X	V	W	X	Y	Z

Carré de Polybe utilisé par le système ADFGX.

Considérons le message « Attaquez demain à quatre heures ». Pour le coder, nous chiffrons chaque lettre selon le carré ci-dessus. Ainsi, A est chiffré FX (ligne et colonne de A dans le carré). Nous obtenons la suite :

FX DX DX FX GX FD AD XX FA AD AX FX AG FF FX GX FD FX DX DF AD AF AD FD DF AD DA

Pour l'instant, nous n'avons donc opéré qu'une simple substitution selon un carré de Polybe. Ce message est maintenant surchiffré au moyen d'une transposition. Celle-ci est déterminée par un mot-clef. Si celui-ci est « nébuleux », nous formons un tableau dont la première ligne est la clef (voir le tableau p. suivante). La deuxième ligne donne l'ordre des lettres de la clef dans l'ordre alphabétique, comme dans le chiffre Übchi. Ensuite, nous copions les lettres du message précédent ligne par ligne. Nous complétons la dernière ligne par des nulles choisies arbitrairement parmi les lettres ADFGX.

N	E	B	U	L	E	U	X
5	2	1	6	4	3	7	8
F	X	D	X	D	X	F	X
G	X	F	D	A	D	X	X
F	A	A	D	A	X	F	X

A	G	F	F	F	X	G	X
F	D	F	X	D	X	D	F
A	D	A	F	A	D	F	D
D	F	A	D	D	A	G	X

Deuxième étape du chiffrement après substitution, mais avant permutation. Celle-ci est toutefois indiquée en deuxième ligne.

Nous écrivons alors les colonnes dans l'ordre donné par la deuxième ligne du tableau et groupons les lettres par cinq pour obtenir le message chiffré :

DFAFF AAXXA GDDFX DXXXD ADAAF DADFG FAFAD XDDFX FDFXF GDFGX XXXFD X

Un coup dur pour l'armée

Le système ADFGX fut usité à partir du 5 mars 1918 et rendit les messages allemands indécryptables. Même s'il était évident que les Allemands allaient attaquer, l'état-major ne savait pas où et fut complètement dérouté par l'offensive du 21 mars. D'autres attaques-surprises suivirent qui, progressivement, asséchèrent les troupes de réserve françaises. Alors qu'au départ, elles étaient échelonnées à l'arrière devant toutes les cibles probables allemandes, il fallait maintenant choisir où les disposer. Heureusement, le 5 avril, Georges Painvin, celui qui était professeur de paléontologie à l'École des mines avant la mobilisation, réussit à percer le mystère !

La présence de cinq symboles faisait penser à un carré de Polybe, donc à une substitution, mais le capitaine avait besoin de la longueur de la seconde clef pour commencer le décryptement. Or les Allemands étaient devenus méfiants, changeaient leurs clefs tous les jours et limitaient l'usage du nouveau système au niveau stratégique. Les tranchées

communiquaient entre elles autrement. La chance arriva le 4 avril, quand Painvin reçut deux messages ayant de fortes similarités. Pour expliquer comment il s'y prit, reprenons notre message dont le texte clair est « Attaquez demain à quatre heures » et chiffrons le texte « Attaquez demain à cinq heures ». Nous obtenons d'abord la suite : « FX DX DX FX GX FD AD XX FA AD AX FX AG FF FX**<u>DD AG FF GX</u>** AF AD FD DF AD DA » où nous avons souligné ce qui diffère par rapport au message précédent. Dans le deuxième tableau les trois premières lignes sont donc identiques et la quatrième également, sauf les deux dernières colonnes.

N	E	B	U	L	E	U	X
5	2	1	6	4	3	7	8
F	**X**	**D**	**X**	**D**	**X**	**F**	**X**
G	**X**	**F**	**D**	**A**	**D**	**X**	**X**
F	**A**	**A**	**D**	**A**	**X**	**F**	**X**
A	**G**	**F**	**F**	**F**	X	D	D
A	G	F	F	G	X	A	F
A	D	F	D	D	F	A	D
D	A	G	X	X	X	X	X

Deuxième tableau avec le message modifié. Les éléments identiques du début ont été soulignés, et nous avons utilisé X pour les nulles.

Une fois les colonnes mélangées, nous obtenons :

DFAFF FGXXA GGDAX DXXXF NDAAF GDXFG FAAAD XDDFF DXFXF DAAXX XXDFD X.

La coïncidence des deux messages en tête s'est transformée en des répétitions toutes les sept lettres (la longueur des colonnes). Découpons les deux messages par groupe de sept pour les mettre en évidence :

DFAFFAA **XXAG**DDF **XDXXX**DA **DAAF**DAD **FGFA**FAD **XDDF**XFD **FXF**GDFG **XXX**XFDX

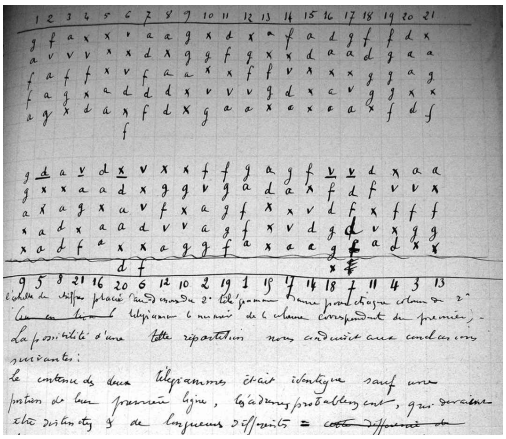
DFAFFFG **XXAG**GDA **XDXXX**FD **DAAF**GDF **FGFA**AAD **XDDF**FDX **FXF**DAAA **XXX**DFDX

Une telle similarité peut être due au hasard, mais c'est peu probable. Georges Painvin sut exploiter une telle occurrence pour en déduire la longueur des colonnes, donc celle de la clef. Il écrivit alors les messages en colonnes et fut ramené au cas que nous avons vu à l'occasion du décryptement des chiffres à transposition. Si les colonnes sont remises dans le bon ordre, une analyse des fréquences des couples de lettres permet de retrouver leur sens, puisque la substitution est mono-alphabétique. Grâce à cette méthode, Georges Painvin réussit à décrypter la moitié des messages allemands.

L'ajout du V : le chiffre ADFGVX

Malgré cela, les Allemands réussirent plusieurs attaques par surprise. Paris n'était plus loin et les réserves françaises s'épuisaient. Le 1er juin, les Allemands changèrent à nouveau de chiffre, ajoutant un V aux cinq autres lettres. Georges Painvin comprit immédiatement que le système n'avait pas réellement changé, que le carré de Polybe avait seulement maintenant un côté de six. 36 symboles composaient donc le tableau. Mais pourquoi utiliser autant de signes ? L'hypothèse naturelle était que les Allemands chiffraient ainsi les 26 lettres de l'alphabet, plus les dix

chiffres. Une apparente complication, qui provoqua en réalité la défaite allemande… En effet, les messages allemands commençaient par l'adresse de l'expéditeur, comme « 15e division d'infanterie » ou « 25e division d'infanterie ». Écrits en toutes lettres, ces en-têtes différaient énormément les uns des autres. Mais le nouveau système amenuisait les distinctions. Entre « 15 » et « 25 », seule la première lettre différait, par exemple.



Manuscrit de Georges Painvin, où il décrit sa découverte de deux messages presque identiques et ses conséquences.

Si le reste des messages était identique, ce qui n'était pas rare, le décrypteur obtenait un renseignement sur la permutation utilisée. En effet, la lettre modifiée en clair se dédouble alors dans le texte chiffré, ce qui permet de pointer les deux premières colonnes (p. suivante en haut).

0	1	2	3	4	5	6	7
10	11	12	13	14	15	16	17
20	21	22	23	24	25	26	27
30	31	32	33	34	35	36	37
40	41	42	43	N	U	L	S

0'	1'	2	3	4	5	6	7
10	11	12	13	14	15	16	17
20	21	22	23	24	25	26	27
30	31	32	33	34	35	36	37
40	41	42	43	N	U	L	S

Points de modification (en gris) dans le tableau d'encodage au niveau du texte non permuté. Cela permet de repérer les deux premières colonnes, ainsi que les dernières si les lettres nulles ne sont pas identiques.

Voici un exemple de deux messages dont les originaux en clair ne diffèrent que sur la première lettre. Avant permutation, ils diffèrent sur les deux premières colonnes. Quand celles-ci sont permutées, elles vont s'éloigner d'un nombre entier de colonnes, donc d'un multiple de leur longueur :

DAXVF AGVXD VFXFX VDDAV D**A**XVX VFGAG FDFXX FAFDD FXDFV VXAXG ADXVF F

GAXVF AGVXD VFXFX VDDAV D**F**XVX VFGAG FDFXX FAFDD FXDFV VXAXG ADXVF F

Comme indiqué précédemment, ces messages diffèrent sur deux lettres. La distance entre ces points de divergence correspond à un certain nombre de colonnes. En comptant les lettres, on trouve qu'elle est égale à 21 : la longueur des colonnes est donc un diviseur de 21. La longueur totale du message est 56. Il s'agit aussi d'un multiple de la longueur des colonnes. On en déduit que la longueur des colonnes est égale à 7 et celle de la clef à 8 ($21 = 3 \times 7$ et $56 = 8 \times 7$). On peut ainsi subdiviser les messages en huit colonnes, que nous écrivons ici en lignes par commodité :

DAXVFAG VXDVFXF XVDDAVD **A**XVXVFG AGFDFXX FAFDDFX DFVVXAX GADXVFF

GAXVFAG VXDVFXF XVDDAVD **F**XVXVFG AGFDFXX FAFDDFX DFVVXAX GADXVFF

Nous pouvons en conclure qu'après substitution, les deux premières colonnes du texte ont été placées en position 1 et 4. Il est probable que la colonne 1 soit devenue la 4 et la 2, la 1. Bien sûr, cela ne suffit pas pour décrypter les messages. Une lettre de plus en tête peut aider davantage, surtout si la première lettre est également modifiée. Les numéros des unités d'une armée se prêtent à ce jeu.

0	1	2	3	4	5	6	7
10	11	12	13	14	15	16	17
20	21	22	23	24	25	26	27
30	31	32	33	34	35	36	37
40	41	42	43	N	U	L	S

A	B	0'	1'	2	3	4	5
6	7	10	11	12	13	14	15
16	17	20	21	22	23	24	25
26	27	30	31	32	33	34	35
36	37	40	41	42	43	N	U

Une lettre de plus en tête décale les colonnes à partir de la troisième. Cela permet de repérer davantage de colonnes. Par exemple, les deux dernières se retrouvent dans les deux premières (mais décalées).

La permutation devient plus claire. Il est possible de repérer la position initiale des colonnes grâce à ces différences. Voici telles qu'elles apparaissent, une fois permutées dans les deux messages :

DAXVFAG VXDVFXF XVDDAVD AXVXVFG **AGFDFX**X **FAFDDF**X DFVVXAX GADXVFF

D**AGFDFX** DFVVXAX GADXVFF A**FAFDDF** XVDDAVD VXDVFXF AXVXVFG DAXVFAG

Les colonnes soulignées représentent les dernières du tableau avant permutation (voir celles qui commencent par A et B dans la figure ci-dessus), donc les colonnes 7 et 8 ont été placées en position 5 et 6. La permutation utilisée se précise. Par ce genre de raisonnement, et beaucoup d'astuce, on finit par la déterminer. L'ordre des colonnes dans le message chiffré est 2, 5, 6, 1, 8, 7, 3, 4. Tous les messages de la journée peuvent alors être mis dans le bon ordre. Ici, cela donne pour le premier message :

AXVXVFG DAXVFAG DFVVXAX GADXVFF VXDVFXF XVDDAVD FAFDDFX AGFDFXX

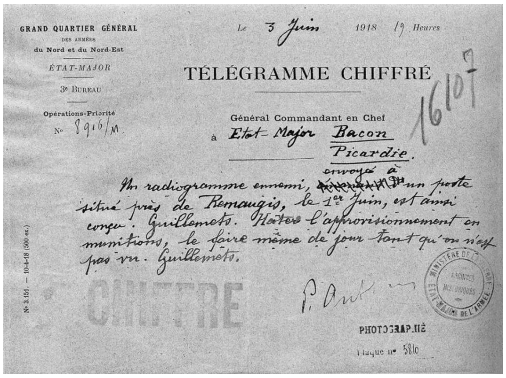
Nous regroupons les digrammes pour obtenir le message avant permutation :

AX VX VF GD AX VF AG DF VV XA XG AD XV FF VX DV FX FX VD DA VD FA FD DF XA GF DF XX

Le même processus est alors exécuté sur tous les messages de la journée, ce qui rend l'ensemble attaquable par la méthode des fréquences et celle du mot probable. Ici, nos messages en clair reprenaient une demande de munitions des 12e, 25e et 115e divisions d'infanterie.

La victoire

Deux messages ayant les particularités que nous venons d'analyser furent interceptés le 1er juin. Georges Painvin les décrypta dès le 2, ce qui lui permit de s'attaquer à l'intégralité des messages de la veille et de découvrir le lieu de la future offensive allemande. Les réserves françaises furent placées exactement où il fallait et, en ce printemps 1918, la victoire qui suivit changea le cours de la guerre. Il devint impossible aux Allemands de surprendre les Français, et cela essentiellement grâce au décrypteur de génie qu'était Georges Painvin.



GRAND QUARTIER GÉNÉRAL
des armées
du Nord et du Nord-Est
ÉTAT-MAJOR
3e BUREAU
Opérations-Priorité
N° 9910/M.

Le 3 Juin 1918 19 Heures

TÉLÉGRAMME CHIFFRÉ

16107

Général Commandant en Chef
à Etat-Major Bacon
Picardie.
envoyé à

Un radiogramme ennemi, [illegible] un poste situé près de Remaugis, le 1er Juin, est annoncé Guillemots. Hâtez l'approvisionnement en munitions, le faire même de jour tant qu'on n'aperçoit pas vu. Guillemots.

CHIFFRE

PHOTOGRAPHIE
Plaque n° 5810

Le « télégramme de la victoire », envoyé suite aux décryptements de Georges Painvin. En indiquant l'emplacement de la future attaque allemande (Remaugis était à une trentaine de kilomètres de Compiègne), il permit aux Alliés de riposter, prélude du succès final.

Ce Qu'il Faut Décrypter

Trois messages en ADFGVX

Les trois messages suivants ont été chiffrés en ADFGVX :

FDDDG GAADF GVGFA AVAAX XFVDA GDADG DAAFF XDFGV GFXDV GDDDA ADDXD GFADD DFDDA D

DAGDA DGDAA GFFXD FGVGF XDVGD DDAAD DXDFA DDDFD DADXF DDDGG AADFG VGFAA VAAXX F

DAGDA DGDAA GFFXD FGVGF XDXGD DDAAD DXDFA DDDFD DADXF DDDGG AADFG AGFAA VAAXX F

On soupçonne qu'ils contiennent le mot « ATTAQUE » et des mots probables comme « DIVISION ».
Où se situe la prochaine offensive ?

Le chiffre de la marine japonaise

Comme les Allemands en 1917, la marine japonaise a surchiffré ses codes durant la guerre du Pacifique. Son chiffre, nommé JN-25 B par les Américains, était composé de trois documents : un livre de code où 45 000 mots ou expressions étaient traduits en nombres à cinq chiffres, et deux livres contenants chacun 50 000 nombres à cinq chiffres qui servaient à surchiffrer. Pour chiffrer un message, le chiffreur partait de la version en codes à cinq chiffres de son message, par exemple :

43321 10063 86172 98151 42711, etc.

Puis il piochait au hasard dans un des livres de surchiffrement une liste de nombres consécutifs, par exemple :

51582 57038 93284 50801 87949, etc.

Il additionnait ces nombres sans retenue pour obtenir le message chiffré :

94803 67091 79356 48952 29650, etc.

Il envoyait ensuite le message avec les références pour que le destinataire retrouve les nombres du surchiffrement. Il restait alors au déchiffreur à retrancher, toujours sans retenue, la liste de nombres au message…

94803 67091 79356 48952 29650, etc.
51582 57038 93284 50801 87949, etc.

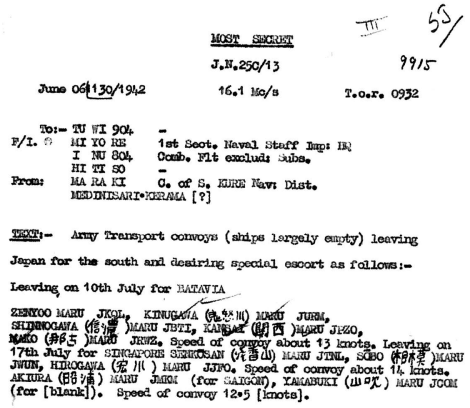
… pour obtenir la liste des codes :

43321 10063 86172 98151 42711, etc.

A priori, ce chiffre aurait été incassable si la liste de nombres en surchiffrement avait été aléatoire car, dans ce cas, il aurait été (quasiment) équivalent à un masque

jetable. Les livres de surchiffrement contenant en tout 100 000 nombres, on aurait pu espérer un chiffre difficile à casser. Malheureusement pour la marine japonaise, pour simplifier un travail fastidieux, les chiffreurs japonais commençaient toujours au même nombre de surchiffrement. Ainsi, le JN-25 B devenait presque l'équivalent d'un livre de codes classique.

Comme nous l'avons déjà vu à propos des chiffres napoléoniens, la solidité d'un chiffre ne dépend pas que des principes sur lesquels il a été bâti, mais aussi et surtout de la façon dont il est manipulé par les chiffreurs. La formation des chiffreurs est un élément essentiel d'un système cryptographique…



MOST SECRET

J.N.25Q/13 9915

June 06 1130/1942 16.1 Mc/s T.o.r. 0932

To:- TU WI 904 -
F/I. ? MI YO RE 1st Sect. Naval Staff Imp: HQ
I NU 804 Comb. Flt exclud: Subs.
HI TI SO -
From: MA RA KI C. of S. KURE Navl Dist.
MEDINISARI•KERAMA [?]

TEXT:- Army Transport convoys (ships largely empty) leaving Japan for the south and desiring special escort as follows:-

Leaving on 10th July for BATAVIA

ZENKOO MARU JKQL, KINUGAWA (衣笠丸) MARU JURM, SHINNOGAWA (信濃川) MARU JUYI, KAINAN (開西) MARU JUZO, MAKO (真光) MARU JUWZ. Speed of convoy about 13 knots. Leaving on 17th July for SINGAPORE SENKOSAN (浅香山) MARU JINL, SOEO (蒼生) MARU JWUN, HIROGAWA (宏川) MARU JJPO. Speed of convoy about 14 knots. AKIURA (秋浦) MARU JMRN (for SAIGON), YAMABUKI (山吹) MARU JGOM (for [blank]). Speed of convoy 12•5 [knots].

Message japonais décrypté par la marine américaine en 1942 : il révèle qu'un convoi vient de quitter le Japon vers le sud.

La transparence du chiffre JN-25 B fut précieuse lors de deux batailles importantes, qui marquèrent le tournant de la guerre du Pacifique : la bataille de la mer de Corail et celle de Midway. Dans les deux cas, les Américains interceptèrent des messages japonais et massèrent leurs forces au bon endroit, ce qui transforma une défaite prévisible en victoire.

Une anecdote intéressante vient agrémenter l'histoire des préparatifs de la bataille de Midway. En plus du chiffrement,

les Japonais employaient des noms de code pour désigner les sites, si bien que les Américains percèrent leurs plans sans être sûrs de l'endroit : ils pouvaient concerner Midway, ou bien un lieu plus au sud dans le Pacifique. La cible de l'attaque était simplement codée « AF ».

Pour lever le doute, un officier demanda au commandant de la base de Midway d'annoncer en clair à la radio qu'il y avait urgence sanitaire, que l'eau potable sur l'atoll manquait suite à un accident à l'usine d'épuration. Arrivé très vite, un message chiffré japonais situa ce problème d'eau potable à « AF », dévoilant où se déroulerait l'attaque nippone : « AF » signifiait donc Midway.

La suite est comparable à la victoire allemande de Tannenberg contre les Russes en 1914. Celui qui croyait surprendre fut surpris… et détruit. Les forces américaines se retirèrent après cette victoire décisive. Le Japon perdit quatre porte-avions, ce qui porta un coup d'arrêt à son expansion et le mit en position défensive, six mois à peine après l'attaque contre Pearl Harbor.

10

Chiffrer avec des instruments artisanaux

Si je vous demande de penser à une machine à chiffrer, je suis prêt à parier que vous venez d'imaginer la grosse boîte ressemblant à une machine à écrire vue dans de nombreux films : l'Enigma allemande de la Seconde Guerre mondiale. Pourtant, elle est loin d'avoir été la seule machine à chiffrer pendant le conflit et encore moins dans toute l'histoire de la cryptographie. Comme nous allons le découvrir, ces dispositifs ont un long passé, remontant au moins au xv^{e} siècle. Ils ont d'abord pris la forme de machines artisanales, appelées cryptographes. Un cryptographe est un instrument, à ne pas confondre avec le cryptologue, la personne spécialiste de cryptographie. Mais, pour l'instant, remontons le temps jusqu'à la Renaissance pour y rencontrer l'une des figures les plus importantes de cette époque d'essor scientifique et artistique.

Un traité de cryptographie

La Rome du xv^{e} siècle. Partout dans la ville jaillissent de terre des ruines romaines, car c'est un âge de redécouverte de la grandeur d'antan, grecque autant que romaine. C'est dans ce milieu effervescent que vit Leon Battista Alberti (1404-1472), à la fois philosophe, peintre, architecte et

mathématicien, comme le voulait l'idéal de la Renaissance. Premier penseur de la perspective, il fut aussi, selon certains historiens, le « père de la cryptographie occidentale ». Théoricien accompli, il inventa de fait la première machine à chiffrer connue, qu'il décrivit en 1466 dans son ouvrage *De Componendis Cifris*, rédigé à peine dix ans après le premier livre imprimé par Gutenberg (1400-1468).

Alberti y évoque précisément « l'inventeur allemand qui, ces temps-ci, est parvenu, en pressant des caractères, à fournir, en cent jours, plus de deux cents volumes de texte à partir de l'original qui lui avait été donné, travail accompli par trois hommes, pas plus ». Dans l'esprit du temps, la diffusion appelle le secret, de sorte que le texte loue dans la foulée « ceux qui, en donnant au caractère un sens tout à fait contraire à l'usage, grâce à leurs techniques pour observer les écritures, que l'on appelle cryptographie, techniques compréhensibles de ceux seuls qui sont dans le secret de la convention, débrouillent et rendent sûr ce que racontent ces textes cryptés ». Cet éloge de l'art du chiffre ne vaudra à Alberti qu'une reconnaissance tardive, sans doute parce que son traité n'a persisté que sous la forme d'une dizaine de copies à peine, avant d'être imprimé en traduction italienne cent ans après sa rédaction en latin.

Le cadran d'Alberti

Dans son traité, Alberti vante ses méthodes, qu'il considère un peu vite comme inviolables :

> Je l'affirme, toutes les intelligences les plus fines et les plus aigües des hommes, tout le zèle des esprits plus vigilants, tout leur art et leurs efforts pour mener des recherches seront trompés.

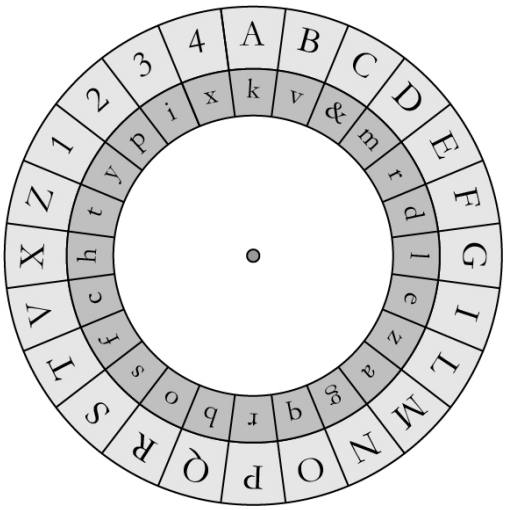
Il dépeint en particulier un objet comportant deux disques concentriques, de tailles différentes, pouvant tourner autour de leur centre commun. Le plus grand est marqué des

lettres de l'alphabet (sauf H, J, K, U, W, Y) et des nombres de 1 à 4. Le plus petit comporte un alphabet de 24 lettres. *A priori*, ce système permet une substitution alphabétique, qui devient poly-alphabétique si on s'autorise à tourner la roue intérieure périodiquement ou non, selon une règle convenue. Il peut servir de multiples manières pour chiffrer. Voici comment Alberti préconise de le manipuler :

> À partir de ce point de départ (l'alignement de *k* et A), chaque lettre du message représentera la lettre fixée au-dessus d'elle. Après avoir écrit trois ou quatre lettres, je peux changer la position de la lettre-indice de façon que le *k* soit par exemple sous le D. Donc, dans mon message, j'écrirai un D majuscule et à partir de ce point, *k* ne signifiera plus A, mais D, et toutes les lettres du disque fixe auront de nouveaux équivalents.

Les nombres de 1 à 4 permettaient d'utiliser un nomenclateur, chaque combinaison de ces quatre nombres ayant une signification comme « pape », « sire » ou « assiéger ». Le cadran d'Alberti constitue donc un chiffre autoclave (rappelez-vous l'autoclave de Cardan, il s'agit d'une façon de communiquer la clef de chiffrement dans le message chiffré lui-même), la clef étant fournie dans le message lui-même par les majuscules.

Bien entendu, ce chiffre ne répond pas au principe de Kerckhoffs, puisqu'il exige le secret du cadran, mais aussi de l'algorithme de chiffrement. Cependant, les correspondants peuvent s'entendre sur un autre mode de fonctionnement qu'ils garderont secret, comme changer la règle d'alignement avec *k*.



Le cadran d'Alberti fait correspondre les lettres de A à Z (sauf H, J, K, U, W, Y), plus les nombres de 1 à 4, à des symboles dans le désordre. Ici, le cadran fait correspondre *k* à A.

Avec la règle donnée par Alberti, on voit qu'un message peut être chiffré de diverses façons, la clef étant donnée dans le message lui-même. Par exemple, le message hautement subversif à l'époque « la terre tourne autour du soleil » peut se chiffrer ainsi avec le cadran d'Alberti :

F*mtqxa*O*mcdkl*I*empcg*E*rebyxb*S*kycbfc*

L'exercice de chiffrement reste assez pénible et sujet aux erreurs. Il est assurément plus simple de privilégier un cadran avec deux alphabets identiques pour chiffrer en Vigenère, comme le faisaient les sudistes pendant la guerre de Sécession.

Ce Qu'il Faut Décrypter

Un message d'Alberti

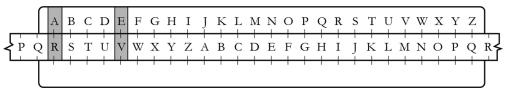
Le message suivant est écrit en français, il est censé venir d'Alberti :

B*zgavx*I*yecmpz*L*zfazm*E*irybk*

Saurez-vous le décrypter ?

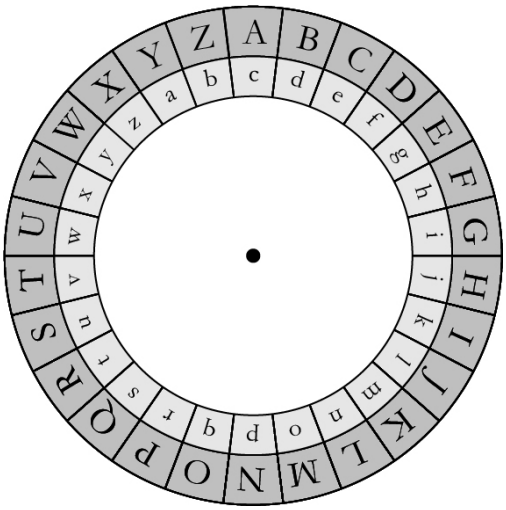
La réglette de Saint-Cyr

L'invention d'Alberti évoque un autre dispositif, certainement le plus simple pour chiffrer en César et en Vigenère : la réglette de Saint-Cyr, du nom de l'école d'officiers de l'Armée de terre où elle était utilisée au XIX^{e} siècle. Elle se présente sous la forme d'une règle munie d'une partie fixe et d'une partie mobile. L'alphabet est écrit une fois sur la partie fixe et deux fois sur la partie mobile.



Réglette de Saint-Cyr. Pour chiffrer la lettre R avec la clef E, on aligne R sous A, puis on lit la lettre chiffrée V sous E.

Pour chiffrer une lettre, on ajuste la lettre-clef de la partie mobile sous le A de la partie fixe. On lit alors directement la version chiffrée de chaque lettre de la partie fixe sur la partie mobile. Il est également envisageable de présenter le dispositif sous la forme d'un cadran légèrement différent de celui d'Alberti. La règle d'utilisation reste la même.



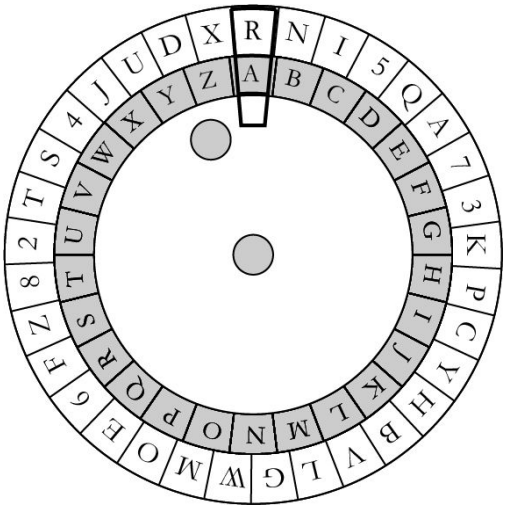
Un cadran pour chiffrer en Vigenère, autre présentation de la réglette de Saint-Cyr.

Les disques de Wadsworth

Les cadrans chiffrants examinés jusqu'ici sont formés de deux disques comportant le même nombre de divisions. Decius Wadsworth (1768-1821), responsable du matériel de la jeune armée américaine, eut l'idée de concevoir un cadran muni de deux disques partagés différemment cette fois. Le disque extérieur contenait 33 caractères (les lettres de l'alphabet, plus les chiffres de 2 à 8) tandis que l'intérieur arborait les 26 lettres de l'alphabet. L'ordre des lettres du disque extérieur était modifiable, car elles étaient gravées sur des plots mobiles. Même si aucun texte source ne l'affirme, le disque intérieur portant l'alphabet usuel correspondait sans doute au texte clair et le disque extérieur au texte chiffré. Ainsi, sur la figure, A serait chiffré en R.

Les deux disques pouvaient tourner autour de l'axe du cadran, de façon connectée grâce à deux engrenages, un de 33 dents pour le disque extérieur et l'autre de 26 dents pour le disque intérieur. Cela signifiait que lorsque le disque intérieur faisait un tour complet, le disque extérieur accusait

un retard de sept cases. Les nombres 26 et 33 étant premiers entre eux, ils n'ont aucun facteur commun, de sorte qu'il fallait 33 tours complets du disque intérieur pour retrouver la même correspondance.



Cadran de Wadsworth, composé de deux disques de 26 et 33 dents, deux nombres premiers entre eux. Ingénieux, il n'a pas été employé en pratique.

Pour utiliser le cadran de Wadsworth, il est nécessaire que les alphabets extérieurs soient les mêmes chez les deux correspondants, bien sûr, mais aussi que ceux-ci s'entendent sur une correspondance initiale des deux disques, comme A et R sur la figure. Pour cela, les engrenages doivent être désembrayés. Cette action est prévue au moyen d'un bouton sur le cadran. On peut alors faire tourner les disques librement.

Cela fait, on embraye les engrenages : les deux disques sont à présent solidaires. On tourne le disque intérieur dans le sens des aiguilles d'une montre, jusqu'à faire apparaître la lettre à chiffrer dans le cadre prévu à cet effet. Le chiffré apparaît dans le cadre au-dessus, on le note et on continue ainsi jusqu'à la fin du message. En somme, cela revient à

utiliser une clef de Vigenère de longueur 33 déterminée par le texte clair.

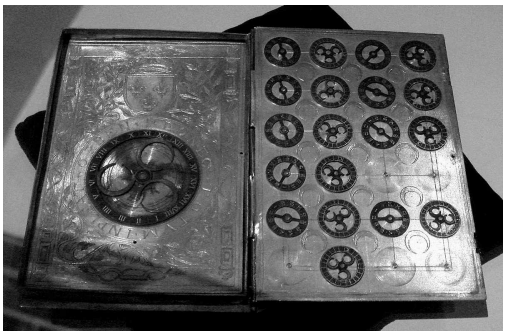
Le cadran de Wheatstone

Le cadran de Wadsworth n'a eu aucun succès, peut-être à cause du décès prématuré de son inventeur. Un dispositif du même genre, mais moins robuste cryptographiquement parlant, a été réinventé de manière indépendante par Charles Wheatstone, cinquante ans plus tard. Le disque extérieur, qui est ici le clair, a 27 caractères (les 26 lettres de l'alphabet dans l'ordre plus un blanc, destiné à la séparation entre les mots) tandis que le disque intérieur (composé des 26 lettres de l'alphabet dans le désordre) constitue la clef du système. Celle-ci se retient comme toutes les clefs de l'époque par un mot ou une phrase. Nous avons déjà vu le procédé avec les carrés de Polybe.

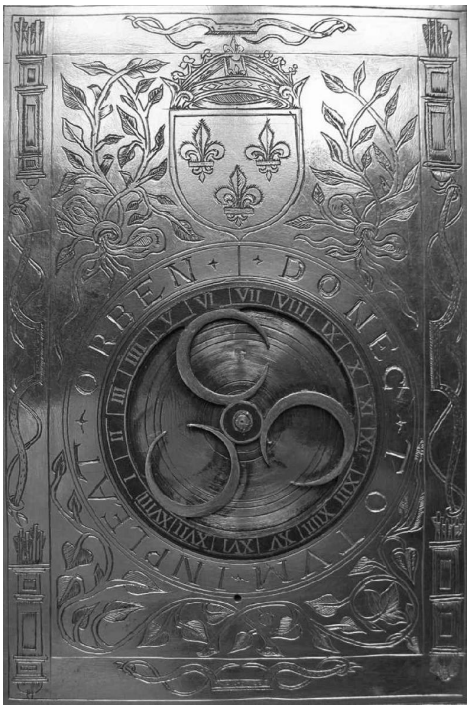
Non seulement passer de 33 à 27 affaiblit le dispositif, mais la procédure prévue par Wheatstone impose de toujours commencer le chiffrement de la même façon. Malgré ses défauts, le cadran de Wheatstone remporta un vif succès quand il fut présenté à l'Exposition universelle de 1867 à Paris. Le colonel Laussedat, membre de la commission française qui examinait la possibilité de l'utiliser pour les communications militaires, fit un rapport très favorable disant que « ce dispositif assure le secret le plus absolu », ce qui était faux car la même substitution se reproduisait périodiquement… Il est attaquable par la méthode de Kerckhoffs que nous avons déjà vue (voir le chapitre 8). De façon ironique, Wheatstone est crédité pour une invention médiocre qui n'est pas la sienne, alors qu'il ne l'est pas pour son invention du chiffre de Playfair (voir le chapitre 4) !

La boîte à chiffrer d'Henri II

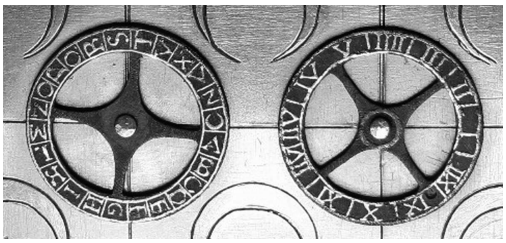
Après ce survol des différents cadrans à chiffrer, revenons en arrière dans le temps avec une boîte mystérieuse, un objet, beau et étonnant à la fois. Elle fut acquise en 1843 par le musée de Cluny, à Paris, en tant qu'instrument astrologique avant d'être reversée au musée de la Renaissance, à Écouen (Val-d'Oise), à sa création en 1977, mais en tant que boîte à chiffrer. On ne sait pas d'où elle vient, ni si elle a servi et à quoi… sauf qu'elle porte le chiffre d'Henri II (1519-1559) : trois croissants entrelacés et l'expression latine *donec totum inpleat orben* (« jusqu'à ce qu'il [le croissant, mais aussi la gloire du roi] remplisse l'orbe entier »). C'est pourquoi le musée de la Renaissance m'avait demandé de l'analyser.



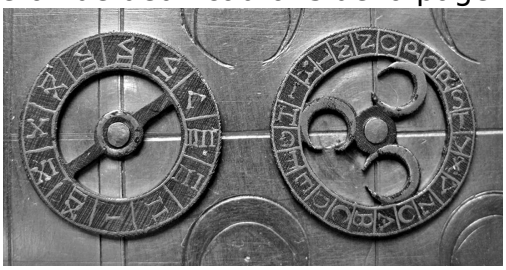
Pages 3 et 4 de la boîte à chiffrer. Cinq cadrans sont manquants.



Page 2 de la boîte à chiffrer, la page 3 est semblable.



Détail de deux cadrans de la page 1.



Détail de deux cadrans de la page 4.

La boîte ressemble en fait à un livre composé de quatre pages. La première page est constituée de 24 cadrans, répartis en quatre colonnes de six. Chaque cadran est une

petite roue dont la jante est divisée différemment selon les colonnes. En colonnes 1 et 3, elle est divisée en 24 angles de 15°, chacun portant l'une des lettres de la suite « ABCDEFGHIKLMNOPQRSTVXYZ » (ce qui fait 23 lettres et non 24, un symbole supplémentaire est décrit plus loin). Les lettres de A à Z sont argentées et inscrites dans le sens de la circonférence (les absences des lettres J, U et W sont classiques, les lettres I et J d'une part et U, V et W d'autre part étant souvent confondues). L'ajout d'un C doré et tourné de 90° est plus original. Il est possible qu'il permette l'utilisation d'un nomenclateur.

La présence de ces cadrans alphabétiques confirme l'hypothèse admise aujourd'hui, selon laquelle cette boîte servait à chiffrer. Par ailleurs, la boîte renferme une multitude de cadrans numériques, deux grands et d'autres plus petits, couplés avec les alphabétiques. De façon assez naturelle, en positionnant le cadran alphabétique sur une lettre et son cadran numérique associé sur un chiffre qui jouera le rôle de clef, on peut chiffrer la lettre selon la clef. Cependant, les essais d'utilisation effective montrent que l'opération n'est guère aisée, car les cadrans sont petits (3,2 cm de diamètre) et les indications le sont encore plus, outre qu'elles sont parfois à moitié effacées – mais cela peut être dû à l'usure du temps.

Plusieurs hypothèses d'action des cadrans numériques sur les cadrans alphabétiques existent, mais toutes difficiles à exécuter avec des doigts d'adultes. Comme ni instruction d'utilisation ni message chiffré avec cet instrument ne sont parvenus jusqu'à nous, nous resterons sur l'idée que cette boîte devait permettre de fournir une substitution poly-alphabétique dont la clef était liée aux deux grands cadrans des pages 2 et 3. Cependant, vu la difficulté de manipulation, il pourrait s'agir avant tout d'un bel objet à montrer, pour impressionner les invités du roi. Les historiens ont envisagé un lien entre le livre et l'astrologie, mais il semble douteux.

La machine de Gripenstierna

Comme on l'a pointé, il n'est pas toujours facile avec la cryptographie et son culte du secret de savoir qui sont les véritables inventeurs. Aux États-Unis, le président Jefferson (1743-1826) est crédité de l'invention du cylindre chiffrant, pourtant la première machine qu'on puisse qualifier ainsi semble avoir été suédoise et plus élaborée que l'américaine ! Il s'agit de l'œuvre de Fredrik Gripenstierna (1728-1804). Il la présenta en 1786 au roi Gustaf III, à qui elle plut, si bien qu'un prototype fut construit.

La machine consistait en 57 roues montées sur un axe. Sur chaque moitié de la circonférence de chacune étaient gravées les lettres de l'alphabet dans l'ordre, et sur l'autre moitié, 26 nombres compris entre 0 à 99, dans le désordre. Le désordre différait pour chaque roue. Le cylindre possédait aussi deux fentes selon son axe, diamétralement opposées, qui donnait sur les roues : l'une dévoilait donc 57 lettres et l'autre 57 nombres.

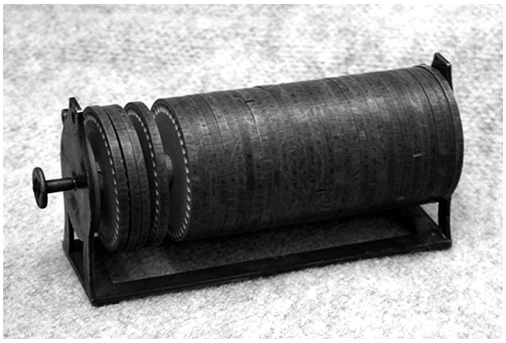
Pour être manipulé, ce dispositif demandait deux opérateurs, un du côté de l'alphabet, l'autre du côté des chiffres. Le premier opérateur faisait tourner les roues pour composer le texte à chiffrer dans la fente devant lui. De l'autre côté, le second notait le texte chiffré. Tous deux recommençaient ainsi par lots de 57 lettres ou chiffres, jusqu'à épuisement du texte à chiffrer. Pour déchiffrer, ils reprenaient l'opération à l'envers. Un seul des deux opérateurs connaissait le secret, celui du côté clair. Gripenstierna avait prévu de commencer le texte avec l'une quelconque des dix premières roues, cette indication étant le premier numéro du message. Pour compliquer un peu plus, le message était envoyé à l'envers, ce qui, à dire vrai, était naturel puisque les opérateurs se faisaient face.

Notez que la séparation en deux opérateurs, un dans le secret et l'autre ignorant, était *a priori* une idée très en

avance sur le temps de Gripenstierna ! En résumé, bien employé, ce cylindre assurait une sécurité supérieure aux cylindres postérieurs que nous présentons plus loin. Ajoutons que l'idée de cylindre chiffrant pourrait être encore antérieure. En effet, de l'aveu même de Gripenstierna, celui-ci avait conçu sa machine sur la base de connaissances acquises auprès de son grand-père, Christopher Polhem (1661-1751). Or ce dernier correspondait avec John Wallis (1616-1703), mathématicien dont le talent de cryptologue s'est exercé durant la révolution anglaise quand il décryptait les messages des royalistes. L'histoire des cylindres chiffrants pourrait donc être plus ancienne qu'on le croit et passer par Wallis…

Le cylindre de Jefferson

Mais revenons au cylindre chiffrant imaginé par le troisième président des États-Unis, Thomas Jefferson. L'idée est de confectionner un certain nombre de disques identiques d'une certaine épaisseur, chacun étant numéroté et portant de façon régulière les 26 lettres de l'alphabet dans le désordre. On les perce au milieu et on peut les assembler dans l'ordre que l'on veut (p. suivante).

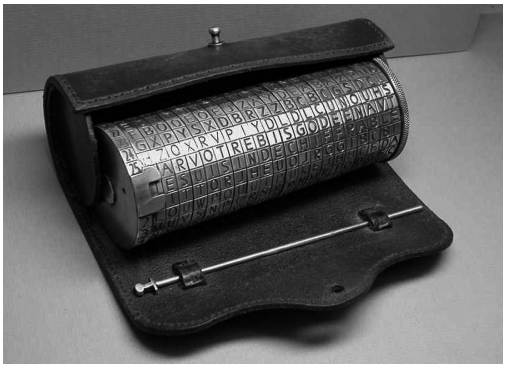


Cylindre de Jefferson. Les roues dentées portent des alphabets dans le désordre. Chacune est numérotée, si bien que leur ordre peut être modifié. Les textes sont lus parallèlement à l'axe.

Le cylindre de Jefferson permet donc un chiffrement par substitution poly-alphabétique, la clef étant l'ordre utilisé pour ranger les cylindres. Pour chiffrer, il suffit de choisir une génératrice du cylindre (l'une des lignes parallèles à l'axe) et de tourner chaque roue de façon à y écrire le message. On lit alors le texte chiffré sur la ligne en dessous ou sur une autre. Pour déchiffrer, il suffit d'écrire les mots chiffrés le long d'une génératrice et de lire le texte au-dessus s'il a été chiffré comme indiqué, sinon on tourne le cylindre jusqu'à trouver quelque chose d'intelligible.

Le cylindre de Bazeries

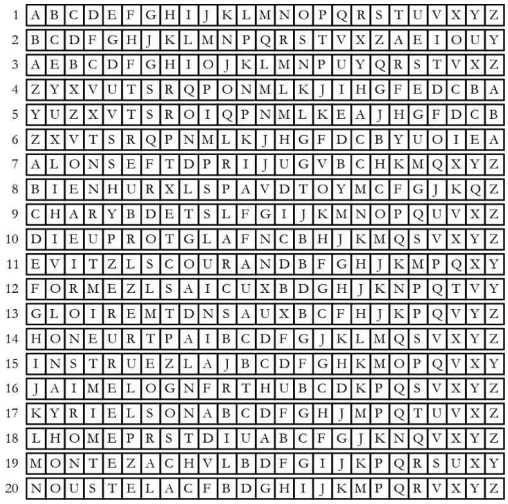
Le cylindre de Jefferson a été réinventé par Étienne Bazeries, qui montra sa machine au ministère des Armées en la présentant comme indéchiffrable. Elle arborait un alphabet de 25 lettres (il n'y avait pas de W).



Cylindre de Bazeries affirmant qu'il est indéchiffrable (voir la ligne du milieu)… ce qui est évidemment faux.

L'armée refusa sa machine avant même que le polytechnicien Gaëtan Viarizio di Lesegno, dit Gaëtan Viaris (1847-1901), montrât comment l'ennemi pouvait la décrypter facilement s'il entrait en possession d'un modèle

– éventualité qui ne doit jamais être exclue, conformément au principe de Kerckhoffs. La méthode de Viaris est fondée sur celle du mot probable.



1	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	X	Y	Z
2	B	C	D	F	G	H	J	K	L	M	N	P	Q	R	S	T	V	X	Z	A	E	I	O	U	Y
3	A	E	B	C	D	F	G	H	I	O	J	K	L	M	N	P	U	Y	Q	R	S	T	V	X	Z
4	Z	Y	X	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A
5	Y	U	Z	X	V	T	S	R	O	I	Q	P	N	M	L	K	E	A	J	H	G	F	D	C	B
6	Z	X	V	T	S	R	Q	P	N	M	L	K	J	H	G	F	D	C	B	Y	U	O	I	E	A
7	A	L	O	N	S	E	F	T	D	P	R	I	J	U	G	V	B	C	H	K	M	Q	X	Y	Z
8	B	I	E	N	H	U	R	X	L	S	P	A	V	D	T	O	Y	M	C	F	G	J	K	Q	Z
9	C	H	A	R	Y	B	D	E	T	S	L	F	G	I	J	K	M	N	O	P	Q	U	V	X	Z
10	D	I	E	U	P	R	O	T	G	L	A	F	N	C	B	H	J	K	M	Q	S	V	X	Y	Z
11	E	V	I	T	Z	L	S	C	O	U	R	A	N	D	B	F	G	H	J	K	M	P	Q	X	Y
12	F	O	R	M	E	Z	L	S	A	I	C	U	X	B	D	G	H	J	K	N	P	Q	T	V	Y
13	G	L	O	I	R	E	M	T	D	N	S	A	U	X	B	C	F	H	J	K	P	Q	V	Y	Z
14	H	O	N	E	U	R	T	P	A	I	B	C	D	F	G	J	K	L	M	Q	S	V	X	Y	Z
15	I	N	S	T	R	U	E	Z	L	A	J	B	C	D	F	G	H	K	M	O	P	Q	V	X	Y
16	J	A	I	M	E	L	O	G	N	F	R	T	H	U	B	C	D	K	P	Q	S	V	X	Y	Z
17	K	Y	R	I	E	L	S	O	N	A	B	C	D	F	G	H	J	M	P	Q	T	U	V	X	Z
18	L	H	O	M	E	P	R	S	T	D	I	U	A	B	C	F	G	J	K	N	Q	V	X	Y	Z
19	M	O	N	T	E	Z	A	C	H	V	L	B	D	F	G	I	J	K	P	Q	R	S	U	X	Y
20	N	O	U	S	T	E	L	A	C	F	B	D	G	H	I	J	K	M	P	Q	R	V	X	Y	Z

Les 20 roues du cylindre de Bazeries (mises à plat). La première donne l'alphabet dans l'ordre, la deuxième et la troisième dans l'ordre un peu modifié, la quatrième dans l'ordre inverse, les cinquième et sixième dans cet ordre inverse modifié. Les autres suivent les phrases : « Allons enfants de la patrie, le jour de gloire est arrivé », « bienheureux les simples d'esprit », « Charybde et Scylla », « Dieu protège la France », « Évitez les courants d'air », « Formez les faisceaux », « Gloire immortelle à nos aïeux », « Honneur et patrie », « Instruisez la jeunesse », « J'aime l'oignon frit à l'huile », « Kyrie eleison », « L'homme propose et Dieu dispose », « Montez à cheval », « Nous tenons la clef ».

Imaginons que nous interceptions un message chiffré ainsi, dont nous supposons qu'il contient le mot « attaque », sans doute sur une ville du Nord : « NLLBE TIVVI UZDLC XEBOI MUAVO ZVTYM RLHPO CTUYR ». Le principe de la recherche du mot « attaque » est simple, même si son application est laborieuse. Examinons comment chaque lettre est chiffrée par chaque roue (voir la figure page suivante).

	A	T	T	A	Q	U	E
1	B	U	U	B	R	V	F
2	E	V	V	E	G	Y	I
3	E	V	V	E	R	Y	B
4	Z	S	S	Z	P	T	D
5	J	S	S	J	P	Z	A
6	Z	S	S	Z	P	O	A
7	L	D	D	L	X	G	F
8	V	O	O	V	Z	R	N
9	R	S	S	R	U	V	T
10	F	G	G	F	S	P	U

	A	T	T	A	Q	U	E
11	N	Z	Z	N	X	R	V
12	I	V	V	I	T	X	Z
13	U	D	D	U	V	X	M
14	I	P	P	I	S	R	U
15	J	R	R	J	V	E	Z
16	I	H	H	I	S	B	L
17	B	U	U	B	T	V	L
18	B	D	D	B	V	A	P
19	C	E	E	C	R	X	Z
20	C	E	E	C	R	S	L

Chiffrement du mot « attaque » pour chaque roue. Dans chaque cas, il suffit de prendre la lettre suivante dans la roue, conformément au tableau ci-dessus.

Cherchons si nous arrivons à reconstituer le début du cryptogramme, soit « NLLBETI » avec ces chiffrements. C'est impossible, car aucune roue n'autorise le chiffrement de T en L ! Essayons donc avec les sept caractères suivants « LLBETIV ». Nous aboutissons à un échec pour la même raison. Poursuivons jusqu'à « IVVIUZD » (à partir de la septième position). Les roues possibles entre les septième et treizième positions se lisent dans le tableau ci-dessus. Nous pouvons les résumer ainsi :

7	**5**	**9**	**10**	**11**	**12**	**13**
12, 14, 16	**2, 3, 12**	**2, 3, 12**	**12, 14, 16**	**9**	**5**	**4**

Positions possibles.

Trois des positions des roues dans le cylindre utilisé pour chiffrer sont déterminées ! Les autres sont questions d'hypothèses. Sans en faire, nous obtenons déjà le décryptement partiel suivant : « NLLBE T **ATTAQUE** LC XEBOI MUAVO ZVTYM **AMI**PO CTUYR ». Il nous faut faire des hypothèses sur les roues 7 à 10 pour aller plus loin, ce qui

est laborieux mais facile, la règle étant que le texte doit avoir un sens. Nous obtenons 14, 2, 3 et 12 dans l'ordre d'où : « NLLBE T **ATTAQUE** LC XEBOI MUAVO Z**SSURAMI**PO CTUYR ». Le « sur Ami… » fait penser que l'attaque se fera sur Amiens, une ville du Nord. Le décryptement continue ainsi. Le message en clair est « Demain, attaquez à quatre heures sur Amiens. Stop. » Cet exemple montre que l'armée a vu juste en n'adoptant pas le cylindre de Bazeries : le choix de l'ordre des lettres sur chaque roue facilite trop le décryptement dès lors qu'on dispose du cylindre.

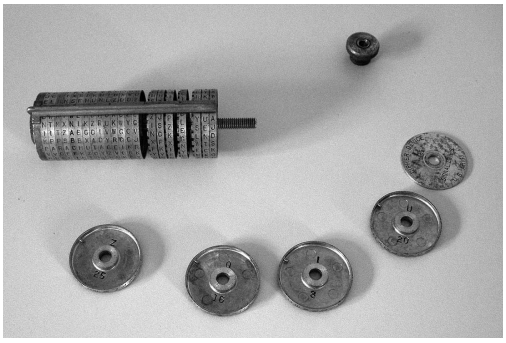
Les carrés latins

Joseph Mauborgne, déjà rencontré à propos du chiffre de Playfair et du masque jetable, découvrit que, pour éviter le décryptement de Viaris, l'idéal était d'utiliser un carré latin, c'est-à-dire un carré où chaque ligne et chaque colonne contient une et une seule lettre, comme dans les grilles de Sudoku, sans que toutefois les lignes se déduisent l'une de l'autre par rotation. Par exemple, il existe quatre carrés latins d'ordre 4 si on écrit la première ligne et la première colonne dans l'ordre :

a b c d	a b c d	a b c d	a b c d
b c d a	b d a c	b a d c	b a d c
c d a b	c a d b	c d a b	c d b a
d a b c	d c b a	d c b a	d c a b

La première est toutefois à exclure, puisqu'il s'agit d'une simple rotation de la première ligne. Grâce à cette idée, Mauborgne améliora le cylindre de Bazeries, appelé à durer puisqu'il fut exploité sous l'appellation M-94 de 1922 à 1943 par l'armée américaine comme machine à chiffrer sur le champ de bataille (la clef était changée quotidiennement).

La M-94 était composée de 25 disques dont l'agencement des lettres tenait compte de l'idée du carré latin et s'exposait moins aux attaques que le cylindre de Bazeries. Seule la roue numéro 17 avait un sens : elle commençait par « the US army ».



La machine à chiffrer M-94 démontée, en usage dans l'armée américaine de 1922 à 1943.

La machine M-94 avec un message.

Ce Qu'il Faut Décrypter

Un message de Machiavel

Le message suivant a été chiffré avec le cylindre de Bazeries :

TRUET FQRNY YUUFQ VIALE NEKBF JRBNS EZNNR UEZV

Sachant qu'il commence par « diviser » et contient le mot « discorde », saurez-vous le décrypter ?

Fascinants, ces cylindres à chiffrer artisanaux préfigurent les machines à chiffrer proprement dites, comme la fameuse Enigma, puisque leurs principes reposent en définitive sur des espèces de rotors. Nous verrons que la mécanique a surtout permis de les faire évoluer vers un usage automatique.

11 Les machines à chiffrer électromécaniques : Enigma et les autres

Après la Première Guerre mondiale, l'augmentation du flot des messages et le retour à une guerre de mouvement réclamaient des transmissions rapides et sûres. C'est sans doute l'une des raisons du développement de la machine Enigma allemande de la Seconde Guerre mondiale. La guerre éclair exigeait une telle machine : il fallait frapper vite et fort en prenant l'adversaire par surprise. Le combat sous-marin reposait sur des exigences similaires, mais pour des raisons totalement opposées : pour coordonner leurs lentes attaques, les commandants de sous-marins devaient à tout prix communiquer entre eux de façon ultrasécurisée.

L'idée de rendre le chiffrement automatique serait donc venue de la lenteur et de la faiblesse des chiffrements manuels de la Première Guerre mondiale. Dans l'imaginaire populaire, la Seconde Guerre mondiale n'a connu qu'une machine à chiffrer, la prouesse allemande. Rien de plus faux. Chaque belligérant avait la sienne. Les États-Unis disposaient de la Sigaba, la Grande-Bretagne de la Typex et la France de la B-211, toutes moins célèbres et pourtant plutôt meilleures que l'Enigma. Ainsi, la Typex comportait 5 rotors tandis que la Sigaba n'en comprenait pas moins de 15 ! Le Japon disposait également d'une machine à chiffrer… que les Américains savaient décrypter dès leur

entrée en guerre, non sans conséquences comme nous le découvrirons bientôt (voir *Le code pourpre*, p. 319).

Ainsi, avec la Seconde Guerre mondiale, le chiffrement change d'échelle ! D'une affaire réservée à une poignée de cryptologues, cette science va se mécaniser et réclamer l'embauche de centaines de spécialistes. Le cabinet britannique de déchiffrement finira ainsi par compter 10 000 personnes…

La machine Enigma

S'il existait de nombreux modèles d'Enigma, tous fonctionnaient sur le même principe. Les plus sophistiqués auraient pu être pratiquement indécryptables par les Alliés si les Allemands n'avaient pas commis quelques erreurs de procédure.

Une Enigma à trois rotors (au fond). Des lampes éclairent le chiffré de la lettre frappée, juste au-dessus du clavier de 26 touches. Le tableau de connexions

occupe la face avant.

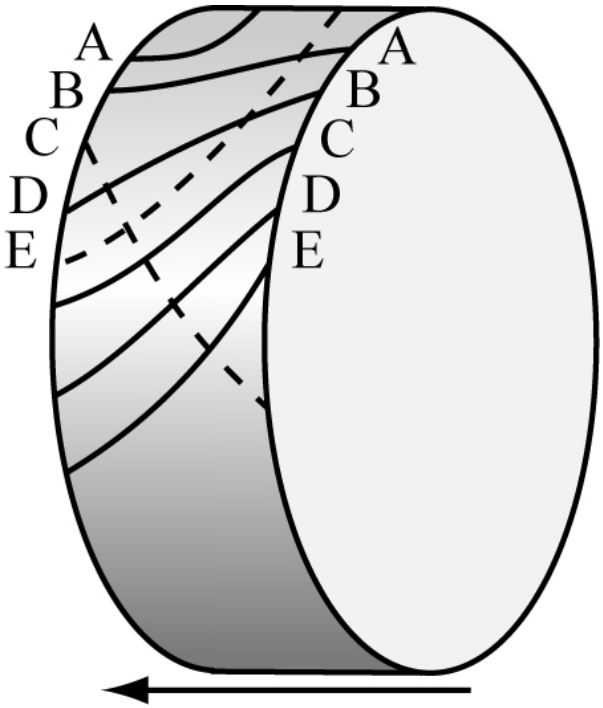
Poste de commandement du général allemand Guderian (debout) pendant la campagne de France, avec une machine Enigma à trois rotors (en bas à gauche) et ses opérateurs au premier plan : un homme pour frapper les touches, un autre pour noter le texte chiffré (qui s'allume à travers les lampes au-dessus du clavier), un radiotélégraphiste pour l'envoyer en morse… plus un officier (à droite) pour surveiller les trois opérateurs !

Arthur Scherbius (1878-1929), le principal concepteur de la machine Enigma, était un spécialiste des moteurs électriques. Son nom est d'ailleurs resté associé aux moteurs asynchrones (ceux qui équipent nos appareils électroménagers ou encore les éoliennes). L'Enigma fut conçue pour protéger les relations commerciales avant d'être adoptée par l'armée allemande. En effet, celle-ci avait compris la faiblesse de ses systèmes de chiffrement de la Première Guerre mondiale et désirait à la fois les améliorer et les accélérer. L'armée se dota ainsi d'environ 100 000 machines entre 1926 et 1945. Si l'Enigma militaire

remporta un succès certain, la version commerciale fut un tel échec que certains se sont demandé si elle n'avait pas été un paravent pour la version militaire, ce qui est fort possible.

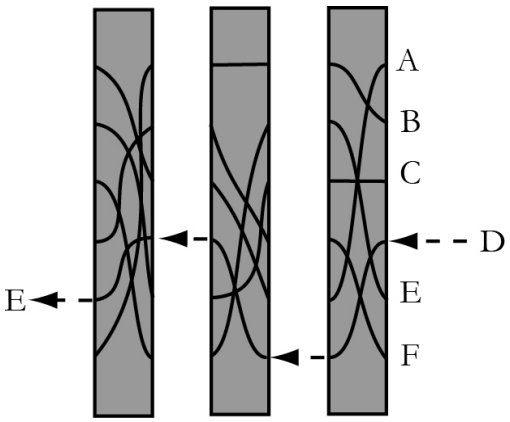
Comment se présente une machine Enigma ? Extérieurement, elle ressemble à une machine à écrire munie d'un clavier de 26 touches représentant les lettres de l'alphabet. En son centre s'alignent des rangées de témoins lumineux. Chaque fois que l'on frappe une touche du clavier, un de ces témoins s'allume et fournit le chiffré de la lettre frappée. La correspondance entre le clavier et les lampes est déterminée, via un système électromécanique, par la position de trois rotors qui coiffent la machine et des fiches d'un tableau de connexions situé sur la face avant. Les trois rotors, associés à un réflecteur dont on verra l'usage plus loin, constituent la partie appelée brouilleur.

Comment fonctionne l'Enigma ? Il s'agit en fait d'une déclinaison sophistiquée du cylindre de Bazeries. Comme les roues du cylindre, chaque rotor de l'Enigma assure une substitution mono-alphabétique, c'est-à-dire une permutation des vingt-six lettres de l'alphabet. La machine Enigma classique en dispose de trois, notés I, II et III. Pour l'améliorer, celles de la marine de guerre allemande en auront quatre, à choisir dans un lot de dix. Les principes restant les mêmes, nous décrirons l'Enigma à trois rotors.



Chaque rotor d'Enigma possède vingt-six crans représentant les lettres de A à Z. Des connexions électriques (fils noirs sur la figure) joignent les crans de droite à gauche, ce qui échange les lettres de l'alphabet. Par exemple, ci-dessus, le rotor III est représenté partiellement : A devient B et B, D, etc.

Pour simplifier, nous figurons chaque rotor sous forme plane avec seulement six crans (de A à F). Plusieurs rotors sont disposés l'un contre l'autre, de gauche à droite, ce qui permet de composer les permutations comme le montre la figure page suivante.



La suite de rotors ci-dessus transforme D en E.

Si elle restait fixe, cette disposition permettrait une seule permutation par texte. Ici, elle correspond au tableau :

$$\begin{pmatrix} A & B & C & D & E & F \\ A & F & B & E & C & D \end{pmatrix}$$

Il signifie que A est changé en A, B en F, C en B, D en E, E en C et F en D. Or un tel chiffre est facile à décrypter grâce à la méthode des fréquences.

Le chiffrement

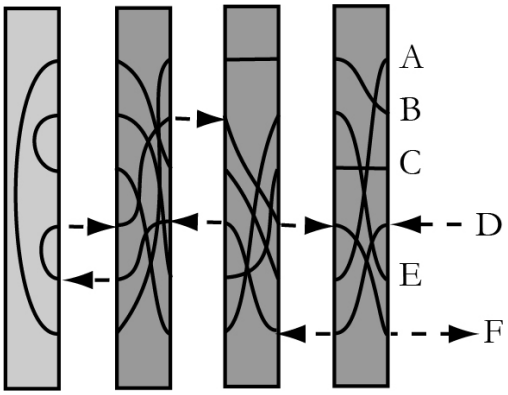
Pour modifier ces substitutions, les rotors se présentent sous forme de petits cylindres, chacun pouvant tourner autour de son axe. Quand on commence à chiffrer un message, ils sont choisis parmi un lot donné (I, II et III), puis placés dans un certain ordre et une certaine position. Ces données forment une partie de la clef. On frappe alors la première lettre. Le premier rotor tourne d'un cran, la permutation des lettres est ainsi modifiée avant que l'électricité ne passe à travers le circuit (des câbles électriques relient les cylindres). Dans notre exemple, elle devient :

$$\begin{pmatrix} A & B & C & D & E & F \\ E & C & A & F & B & D \end{pmatrix}$$

Quand on frappe la deuxième lettre, le rotor tourne à nouveau. Quand il a tourné de vingt-six crans, le deuxième rotor tourne d'un cran, et ainsi de suite.

Le réflecteur

À l'extrémité des rotors se trouve un dispositif nommé réflecteur. Son objectif n'est pas d'apporter de la complexification au chiffrement, au contraire, cet élément vise à faciliter le déchiffrement pour le destinataire du message. Le réflecteur renvoie le signal vers l'entrée du premier rotor. Il assure la symétrie du fonctionnement de la machine : si une lettre X est transformée en Y, alors Y est transformée en X. Autrement dit, une même Enigma, sans changement de sa configuration, peut servir au chiffrement et au déchiffrement du même message.



Le brouilleur d'une Enigma : le réflecteur (à gauche) sert à réfléchir le signal. Le déchiffrement se fait ainsi avec la même machine dans la même disposition puisque, si D donne F, alors F donne D.

Connexions des rotors de l'Enigma à trois rotors

Par commodité, nous représentons les rotors à plat, la partie droite en haut. Les connexions sont alors données par les tableaux suivants :

A	B	C	D	E	F	G	H	I	J	K	L	M
E	K	M	F	L	G	D	Q	V	Z	N	T	O

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
W	Y	H	X	U	S	P	A	I	B	R	C	J

Rotor I

A	B	C	D	E	F	G	H	I	J	K	L	M
A	J	D	K	S	I	R	U	X	B	L	H	W

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
T	M	C	Q	G	Z	N	P	Y	F	V	O	E

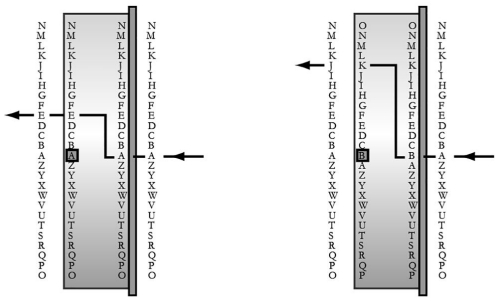
Rotor II

A	B	C	D	E	F	G	H	I	J	K	L	M
B	D	F	H	J	L	C	P	R	T	X	V	Z

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
N	Y	E	I	W	G	A	K	M	U	S	Q	O

Rotor III

Ces tableaux correspondent au positionnement des rotors sur la lettre A. Par exemple, pour le rotor III positionné sur la lettre A, la lettre A est transformée en B, B en D, etc.



Le rotor I en position A à gauche et en position B à droite. La permutation de l'alphabet est modifiée.

Si nous positionnons le rotor III sur la lettre B, nous devons tout décaler d'un cran, mais les connexions internes restent les mêmes puisqu'il s'agit d'un câblage physique. Les connexions sont alors données par le tableau suivant. Les deux lignes du milieu (en gris) représentant le câblage physique sont identiques au tableau précédent.

A	B	C	D	E	F	G	H	I	J	K	L	M
B	C	D	E	F	G	H	I	J	K	L	M	N
D	F	H	J	L	C	P	R	T	X	V	Z	N
C	E	G	I	K	B	O	Q	S	W	U	Y	M

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
O	P	Q	R	S	T	U	V	W	X	Y	Z	A
Y	E	I	W	G	A	K	M	U	S	Q	O	B
X	D	H	V	F	Z	J	L	T	R	P	N	A

Le réflecteur correspond à une permutation fixe.

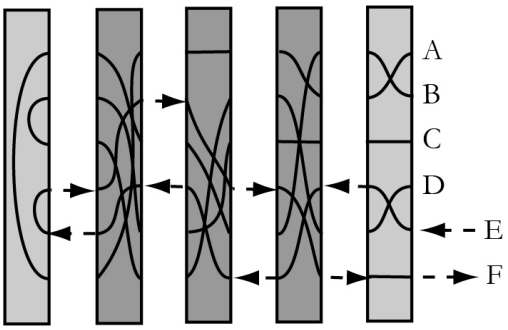
A	B	C	D	E	F	G	H	I	J	K	L	M
Y	R	U	H	Q	S	L	D	P	X	N	G	O

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
K	M	I	E	B	F	Z	C	W	V	J	A	T

Les connexions du réflecteur.

Les modèles les plus évolués de la machine Enigma proposaient un choix entre quatre réflecteurs, mais nous continuerons notre analyse avec le modèle classique.

Pour compliquer le système de chiffrement d'Enigma, un tableau de connexions est placé au début du dispositif précédent. Dans le modèle classique, il permet d'échanger douze lettres au moyen de six fiches. Il sera porté à dix fiches dans les modèles les plus évolués.



Le fonctionnement d'Enigma : si on frappe E, F s'allume et vice-versa. Le tableau de connexions est à droite, le réflecteur à gauche et les rotors au centre.

Les livres de clefs

Comment utilisait-on concrètement une machine Enigma ? Au préalable, il importait de partager une clef secrète avec son destinataire, afin que la machine de déchiffrement soit configurée comme celle qui a servi à chiffrer le message. Dans la pratique, l'armée allemande disposait d'une clef par jour. Ce système de clefs devait être tenu secret, sinon tous les messages pouvaient être décodés avec n'importe quelle Enigma. La clef regroupait en fait plusieurs informations nécessaires au fonctionnement du dispositif. Tous les mois, les forces allemandes recevaient de nouveaux livres de clefs comportant les combinaisons pour chaque jour.

Quelles informations comportait la clef ? Eh bien, la position des six fiches du tableau de connexions, le choix et l'ordre des rotors et la position initiale de chaque rotor, cette position étant repérée par une lettre de l'alphabet. Sans le tableau de connexions, le nombre de clefs possibles serait relativement faible. Choisir l'ordre de trois rotors ne donne que six possibilités : I II III, I III II, II I III, II III I, III I II et III II I. Fixer la position d'un rotor revient à piocher une lettre de l'alphabet, soit 26 possibilités. Et en choisir trois donne 26 × 26 × 26, ce qui multiplié par 6 fournit 105 456

configurations de rotors différentes. Ce nombre semble énorme, mais il est plutôt raisonnable dans ce contexte.

C'est alors que le tableau de connexions change tout, puisqu'il dispose de six fiches, chacune devant réunir deux lettres pour les échanger (ainsi, si on connecte les lettres A et I, quand on appuie sur la touche A, c'est comme si on appuyait sur I… et de même en sortie). Pour enficher la première fiche du tableau de connexions, nous devons choisir une première lettre parmi 26 et une deuxième parmi 25. Cela fait *a priori* 26 × 25 possibilités, mais, comme chacune se retrouve deux fois, nous obtenons 325 façons de placer la première fiche. Avec ce type de raisonnement, on arrive au nombre vertigineux de 10 586 916 764 424 000 configurations. Plus de dix millions de milliards !

On le comprend, la difficulté de décrypter Enigma tient au tableau de connexions, pas à la partie brouilleur (les rotors associés au réflecteur). L'une de ses faiblesses se situe là également, car le tableau de connexions n'opère pas sur toutes les lettres. Son autre défaut est qu'une lettre ne peut jamais être changée en elle-même, comme dans le cylindre de Bazeries.

Poursuivons le chiffrement, sans utiliser le tableau de connexions pour simplifier. En positionnant les rotors de gauche à droite (I, II, III chacun sur la lettre A), on transforme le message : « Une machine peut-elle être indécryptable ? » en :

ZQCOO MTBVC QTVAS XBZOS PPVQV ZUXQG AGKWZ

Comme toujours, tous les signes de ponctuation sont éliminés ou remplacés par des groupes de lettres peu courantes comme « XX » ou « XY », et les lettres sont groupées par cinq. Tout cela est ensuite transmis en morse via les ondes radio.

Après avoir considéré les actions des trois opérateurs en charge de la machine (voir l'illustration avec le général Guderian), voyons concrètement comment s'effectue le

chiffrement de la première lettre par la machine. On frappe U sur le clavier, le rotor III tourne d'un cran et U se transforme en L qui, avec le rotor II devient H puis avec le rotor I, Q. Le réflecteur transforme Q en E. Le rotor I opère maintenant à l'envers, E devient A, A reste A avec le II et A devient Z avec le III (voir les connexions des rotors et du réflecteur). Pour déchiffrer ce texte, il suffit de disposer d'une Enigma configurée de la même façon. C'est également l'idée de base du décryptement sans connaissance de la clef.

Il faut casser Enigma

[210] Le premier décryptement d'Enigma fut un succès conjoint de l'espionnage français et du génie de trois mathématiciens polonais : Marian Rejewski, Jerzy Rozycki et Henryck Zygalski. Un fonctionnaire allemand du bureau du Chiffre, Hans-Thilo Schmidt (1888-1943), en trahissant son pays pour de l'argent jusqu'à son exécution en pleine guerre, a fourni une aide précieuse. Il a dévoilé les tables de chiffrement et les consignes d'emploi de l'Enigma de l'armée allemande de 1931 à 1938, et bien d'autres renseignements ensuite. C'est grâce aux informations fournies par Schmidt qu'on a pu reconstituer les câblages de la version militaire de l'Enigma puis en fabriquer des répliques, et ce dès 1933.

Le mathématicien polonais Marian Rejewski (1905-1980) contribua grandement à « casser » Enigma dans les années 1930.

Il faut préciser qu'une erreur de procédure allemande a facilité ce travail de reconstruction. Les chiffreurs avaient en effet pour habitude d'indiquer les positions initiales des rotors, par exemple « RAS », en début de message. Or, pour éviter toute erreur de transmission, ils répétaient les trois lettres, ce qui donnait « RASRAS ». Les deux R, les deux A et les deux S étaient ainsi chiffrés de façon différente selon la position du rotor de droite, trahissant par là une partie de son câblage…

Cette erreur a ouvert une voie d'attaque mathématique de l'Enigma liée à la théorie des groupes d'Évariste Galois (1811-1832)… un sujet théorique très éloigné *a priori* du décryptement des messages de l'armée allemande. Grâce à leur maîtrise de cette théorie fort abstraite, les Polonais se trouvaient en possession de répliques de l'Enigma militaire. Avec les tableaux de clefs, ils étaient donc à même de décrypter les messages allemands.

La *bomba*

Les mathématiciens polonais tentèrent de se passer des tables de chiffrement, car ils se doutaient qu'un jour ou l'autre l'espion se ferait prendre ou serait écarté par le hasard d'une mutation. Ils réussirent à le faire, en particulier en créant une machine, la *bomba*. Elle permettait de trouver la clef du jour en quelques minutes seulement. Ce sont les fameuses « bombes », dont l'invention est souvent attribuée aux Anglais alors qu'ils en ont hérité. Le mérite de ces derniers est d'avoir su les perfectionner pour suivre les évolutions d'Enigma. En particulier, périodiquement, les Allemands ajoutaient de nouveaux rotors à la machine et obligeaient les mathématiciens à revenir à leur table de travail pour déterminer rapidement leur nature.

La capture providentielle de deux sous-marins allemands les aida. Le 9 mai 1941, l'*U-110* fut abandonné par son équipage alors que son capitaine pensait être éperonné par le *Bulldog*, le destroyer qui le poursuivait. Le commandant du *Bulldog* eut l'intelligence de se contenter d'accoster le sous-marin et d'arrêter l'équipage, avant de faire fouiller le navire. On y trouva une Enigma, ses rotors et la clef du jour. L'*U-110* fut ensuite coulé pour que les Allemands ne se doutent pas de ces prises.

La capture de l'*U-110* par le *Bulldog* en mai 1941 fournit une machine Enigma et de nombreux éléments attenants.

En février 1942, les Enigma de la Kriegsmarine passèrent à quatre rotors, ce qui rendit les messages des sous-marins à nouveau indécryptables. Heureusement, des erreurs de procédures permirent aux Britanniques d'en trouver les câblages. La capture de l'*U-559* le 30 octobre 1942, avec une de ces nouvelles Enigma à son bord, permit de compléter les câblages esquissés. L'épisode fut dramatique, puisque deux des marins britanniques qui pénétrèrent dans le sous-marin endommagé, pour y récupérer le matériel cryptographique, ne purent en sortir avant qu'il ne coule.

Bienvenue à Bletchley Park

Les Britanniques industrialisèrent **[220]** le renseignement, dont le décryptement devint l'une des composantes majeures à l'instigation de Winston Churchill (1874-1965). De par son rôle dans la conduite de la Première Guerre mondiale, Churchill connaissait l'importance du décryptement des dépêches ennemies. L'équipe de spécialistes qui concentra les efforts britanniques en la matière fut réunie au début de la guerre à Bletchley Park, un manoir situé à 80 kilomètres au nord-ouest de Londres. À la fin de la guerre, elle comprenait 10 000 personnes environ, dont 80 % de femmes, des mathématiciens, des linguistes et même six cruciverbistes, recrutés en 1942 par un concours organisé par le *Daily Telegraph* ! Pour maintenir la confidentialité sur les activités du lieu, tous les renseignements issus des équipes, lors de leur transmission aux Alliés, étaient présentés comme venant d'une source fictive nommée *Ultra*.

Alan Turing (1912-1954). Avant-guerre, il s'occupait de logique et de fondements des mathématiques, des sujets qu'on pourrait croire loin des applications qui firent sa gloire.

L'éloignement de Londres et des centres industriels mettait Bletchley Park à l'abri des raids aériens allemands. Le manoir restait cependant proche du chemin de fer et des réseaux téléphonique et télégraphique. Un jeune mathématicien issu de l'université de Cambridge, Alan Turing, y dirigeait la section du service chargée de décrypter les messages de la marine allemande. Au sein de Bletchley Park, ce service fut celui qui eut le plus d'impact sur le cours de la guerre.

La procédure de décryptement moderne

Avant de voir comment Alan Turing réussit à percer les secrets allemands, examiner comment nous pourrions le faire avec les moyens modernes va nous aider à

comprendre la logique mise en œuvre par le mathématicien. Voici un message chiffré avec une machine Enigma à trois rotors :

CDZWO DJUBF HBYUX AMRUE JGDJL QCLVZ WKJVU PBCNA HCGDS WSUQS LFOEH FBPSK QYKWD ZKJAP JIKHA FAAOP CTEPZ QZLJQ CBHCG OYNSF WRYBR WAQYJ RTHDX ERNKH NLUDB HVLET ZCFMK HTZZW DRSKW MOQPG HERNI WRFXH FXJQT BWVTH QMWBQ SLWLS IHINM JGFZC MISHO TSQDS TEZSY FSITZ FWUKK TWKID JJUKJ EBALH LHXMO CXMWZ NJDHG PVFZH VJJZM VNWK

Pour le décrypter, il suffit de trouver dans quelle position se trouvaient les rotors et le tableau de connexions au début de son chiffrement. Pour ce faire, on pourrait essayer toutes les possibilités au moyen d'un ordinateur et ne retenir que celles fournissant des fréquences compatibles avec la langue utilisée. En théorie, c'est susceptible de fonctionner, mais en pratique, le nombre de possibilités est bien trop grand en raison du tableau de connexions.

Pourtant, c'est là que se situe la faille d'Enigma. Ce tableau ne permute que douze lettres deux à deux. Autrement dit, quatorze sont inchangées (par les connexions des fiches). Ainsi, dès lors que nous perçons la bonne disposition des rotors, un certain nombre de lettres sont à leur place : toutes celles qui n'ont pas rencontré une des lettres modifiées du tableau de connexions. Si le message est suffisamment long, cela se retrouve dans les calculs statistiques le concernant, comme nous allons le voir.

La position des rotors

Pour déterminer la position des rotors, nous allons utiliser six ordinateurs, chacun correspondant à un ordre des trois rotors. Chacun génère les positions des rotors de A à Z, l'une après l'autre. On chiffre le message avec cette position sans utiliser le tableau de connexions. Dans chaque cas, on calcule alors l'indice de coïncidence du résultat (voir p. 246). Par exemple, pour l'ordinateur simulant une Enigma

avec les rotors dans l'ordre I, II, III, chacun étant sur la lettre A, on trouve :

QAAEA VBDFQ XFZWJ CNOBP ZYFCG PUOZH DDFFC NLIEN KPNUZ HWVBX VOBXN JVUXB SLQGW MRKOH QDEMT ASORW ZKHOQ MWNUP FGIFQ XVIUT BIHJN IBMNB VJKRW OTGDS MHZHA FUQYL QLUEU CDBXD WJCGL ZMIBI CKBYL LCSGB EGMDJ ZUTZB GQIKR ZAYFX RKLBV SUVHU POXFE MKKUE OZCHS RIQCF ESACS INSMV TAXHU JHOZV HFDAR QOBJY OURFU OJCRY SFUNI TFFC

Son indice de coïncidence est 0,0378. On effectue ensuite le même calcul avec les 17 576 positions des rotors possibles et on garde le record, c'est-à-dire celui qui donne l'indice le plus grand. On compare les records des six simulateurs, ce qui fournit l'indice 0,0508 pour les rotors dans l'ordre III, I, II réglés aux lettres B, Y et D. Le nouveau texte est :

ATANJ CEOET RYMTK JSLMH NENUV JDQDA NSESN YAUKE REARN STDWR MGUAL LREMT IGRLB HNERX AWITB BRJGK LIDVJ SUPSW TALAU JTJNL CESSL IODEI TRETY YMDEU FDEAO EMOYM TEISS XUNPE BERLO VTJOV VREYL CEWBR XRLHR YMSDG KEMHB EPUAI BNWLS EIALS LJITB LRTYP ETHDO AOPSV EEXUE ICEBQ EAAEO UPENM IDRQF ATFTC CAGEO SAZDN CCNOQ RYES

A priori, le résultat n'est guère plus parlant ; pourtant, nous nous sommes approchés de la solution. Comme toujours, décrypter est affaire de patience. Continuons en supposant que nous avons bel et bien trouvé les bonnes positions des rotors, même si rien encore ne le confirme.

Le tableau de connexions

Pour disposer le premier câblage, nous avons 325 possibilités qu'il nous faut toutes essayer. Nous trouvons que la connexion IN optimise l'indice de coïncidence avec le texte :

ATAIJ CEOET RYMTK JSLMH IEIUV JDQDA ISESI YAUSE REARI STDWR MGUAL LREMT NGRLB HIERX ALNTB BRJGK LNDVJ SUPSW TALAU JTEIL CESSL NODEN TRETY YMTEU RDEAO EMOYM TENSS XUIPE BERLO VTJOV VREOE CEWBR XRLHR YMSDG KEMHB EPUAN TIXUS ENALS LLNTB LRTYP ETHDO AOESV EEXUE NCESQ EAAEO UPEIM NDRQF ATFTC EAGEO SAZDI CCIOQ RCES

dont l'indice est égal à 0,0559. En recommençant, nous trouvons la connexion MP et le texte :

ATAIJ CEOE T**RYPT**KJ**R**L**PHIE** IUV JDQDA ISESI AAUSE REARI STDWR PGUAL LRYPT NGRLB HIERE ALNTB BRJGE LNDSJ SUMSW TALAU JTEIL CESSL NODEN TRETY YPTEU RDEAO EPOYP TENRS XUIME BERLO UTJIV VREOE CEWBR XRLHR YPSDG KLPHB EMUAN TIXUE ENALS SLNTB LRTYM ETHDO AOESV EEXUE NCESQ EAAEO UMEIP NDRLF ATETC EAGEO EAZDI CCIOE RCES

dont l'indice de coïncidence est égal à 0,0613.

Changeons maintenant de tactique, car la plupart des lettres importantes sont en place. Le troisième groupe du texte, celui que nous avons repéré en gras, semble suffisamment clair : il doit s'agir du mot « cryptographie ». On comprend l'intérêt d'inclure des cruciverbistes dans l'équipe de déchiffreurs ! Cette idée invite à essayer la connexion AL. En continuant ainsi, nous trouvons successivement les connexions FV, QX, puis DO et enfin le message : « le livre de cryptographie que vous lisez illustre l'histoire de la cryptographie de l'Antiquité à nos jours et la lutte incessante entre chiffreurs et décrypteurs qui mènera du chiffre de César à la cryptographie quantique en passant par la méthode des fréquences, celle du mot probable et celle des coïncidences ».

Le décryptement de Turing

Même si les Britanniques avaient envisagé la méthode, cet algorithme de décryptement d'Enigma était inutilisable à l'époque de la Seconde Guerre mondiale. La capacité de calcul était alors insuffisante. Alan Turing ne put donc se servir de la méthode des coïncidences pour casser les messages d'Enigma. À la place, il employa la méthode des mots probables. Comme nous l'avons déjà noté, ceux-ci peuvent être « divisions », « quartier général » ou tout simplement « bulletin météo », voire ce bulletin même.

Comment Turing procède-t-il ? Tout d'abord, il localise les mots probables en repérant les lettres qui diffèrent. Il dispose alors d'un texte et de son chiffrement, par exemple : « DUHAU TQUAR TIERG ENERA L » et « ANOTC FLNLF

GOPEN SUTQP M ». Il exploite ensuite ce couple pour trouver la disposition des rotors et du tableau de connexions de l'Enigma, valable pour le jour donné puisque les clefs changeaient quotidiennement, à minuit. Dans ce qui suit, nous utilisons une Enigma à trois rotors, sachant que les principes restent valables pour les modèles à quatre rotors. Dressons le tableau de correspondance des lettres dans notre premier exemple :

1	2	3	4	5	6	7	8	9	10	11
D		H	A	U	T	Q		A	R	T
	U						**U**			
A		O	T	C	F	L		L	F	G
	N						**N**			
12	13	14	15	16	17	18	19	20	21	
I	E	R	G	E		E	R	A	L	
					N					
O	P	E	N	S		T	Q	P	M	
					U					

Correspondance des lettres à chaque étape du chiffrement.

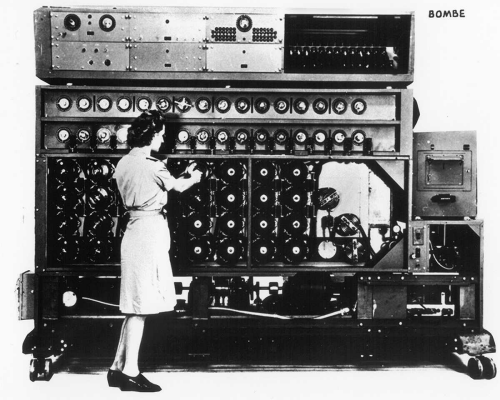
Les paires ont été soulignées.

Certaines lettres se correspondent plusieurs fois, ici U et N, deux fois dans un sens et une fois dans l'autre – ce qui revient au même puisque Enigma chiffre de façon symétrique. Comme toutes les lettres ne sont pas échangées par le tableau de connexions, on peut supposer

que U et N ne le sont pas, et voir les conséquences de cette hypothèse.

Bombes cryptographiques

Pour appliquer cette méthode, il est nécessaire de pouvoir faire fonctionner un grand nombre de machines Enigma ensemble et automatiquement. Les machines qui réalisaient cette opération au temps de la Seconde Guerre mondiale portaient le nom de « bombes » à cause du bruit qu'elles produisaient. Deux cents d'entre elles furent construites pendant la guerre. Pour les faire fonctionner, il fallait les câbler selon les paires ou les cycles trouvés. Les machines n'indiquaient pas directement la position des rotors utilisée, mais des positions impossibles. Il fallait ensuite en déduire manuellement la position correcte.



Une bombe. Les roues servent aux réglages.

Dans notre exemple, pour chaque position, nous essayons toutes les configurations des rotors pour ne retenir que celles échangeant U et N en deuxième, huitième et dix-septième positions (voir le tableau p. suivante). Nous

trouvons ainsi que les rotors sont en position III, I, II et réglés sur les lettres A, D et Y.

Bien sûr, la méthode ne fonctionne pas toujours. Premièrement, il est possible que nous ne trouvions aucune paire. Il est possible aussi qu'elles donnent un grand nombre de possibilités de disposition des rotors. Cependant, si nous identifions plusieurs paires dans plusieurs messages, il est probable que cela coïncide avec la disposition des rotors.

Prenons un autre cas :

« DUHAU TQUAR TIERG ENERA L » est chiffré en « OXUEV ADQHT HGTFC XADEO I »

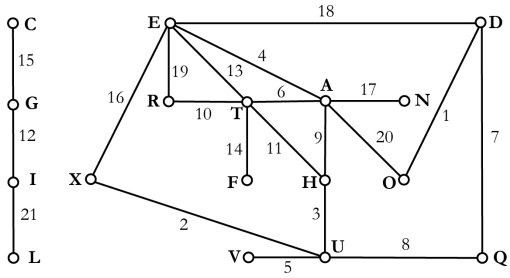
Nous obtenons ainsi un tableau sans paire… qui ne révèle pas grand-chose sur la correspondance trouvée !

1	2	3	4	5	6	7	8	9	10	11
D	U	H	A	U	T	Q	U	A	R	T
O	X	U	E	V	A	D	Q	H	T	H

12	13	14	15	16	17	18	19	20	21
I	E	R	G	E	N	E	R	A	L
G	T	F	C	X	A	D	E	O	I

Correspondance des lettres à chaque étape du chiffrement.

Il est beaucoup plus intéressant de la représenter sous la forme d'un graphe, en reliant les lettres par des arcs que l'on marque par le numéro de l'étape du chiffrement.



Graphe représentant les correspondances des lettres entre le message et son code. Par exemple, D est relié à O à l'étape 1, O à A à l'étape 20, A à N à l'étape 17, etc.

Ce graphe est manifestement composé de deux parties. Celle de gauche n'a guère d'intérêt. En revanche, celle de droite, avec ses nombreux cycles, est pleine d'enseignements. Imaginons pour commencer que A (au centre de la figure) soit inchangé. Essayons toutes les dispositions des rotors telles que A soit changé en une lettre en sixième position, elle-même changée en une autre lettre en onzième qui est changée en A en neuvième (voir le cycle de A au centre de la figure). Ici, nous ne trouvons aucune solution. Nous recommençons en échangeant A avec les autres lettres de l'alphabet. En tenant compte des autres cycles, nous trouvons que les rotors sont en position III, I, II et réglés sur B, D et Q. La technique donne simultanément le tableau de connexions. Ici par exemple, A est échangé avec V, E avec T, H avec Y, J avec F, L avec P et D avec W.

Les lettres qui diffèrent

Pour mettre en œuvre ce qui précède, encore faut-il trouver la position du mot. Une particularité d'Enigma rend la tâche possible : à cause du réflecteur, aucune lettre n'est chiffrée en elle-même. Faisons donc défiler les mots probables comme « panzer » le long du texte et cherchons un cas sans coïncidence. Il est possible alors que nous

ayons trouvé une occurrence de notre mot. Bien entendu, cela fonctionne mieux avec des mots longs que des mots courts. L'armée allemande en fournissait beaucoup, en particulier dans les messages météo. Par exemple, considérons le message : « TJNWU TBIMQ WMYIC CGNDD DUIXW MXNZN NRTP ». Cherchons-y le mot probable : « BULLETIN METEO NORD ATLANTIQUE ». Pour cela, mettons-les en correspondance.

T	J	N	W	U		B	I		Q	W	M	Y	I
					T			**M**					
B	U	L	L	E		I	N		E	T	E	O	N
					T			**M**					
C	C	G	N	D	D	D	U	I	X	W	M	X	N
O	R	D	A	T	L	A	N	T	I	Q	U	E	

Première mise en correspondance.

Les deux coïncidences soulignées rendent cette position impossible. Nous continuons ainsi en décalant le mot probable.

T	J	N	W	U	T	B		M	Q	W	M	Y	I
							I						
	B	U	L	L	E	T		N	M	E	T	E	O
							I						
C	C	G	N	D	D	D	U	I	X	W	M	X	N
N	O	R	D	A	T	L	A	N	T	I	Q	U	E

Deuxième mise en correspondance.

Une coïncidence rend à nouveau cette position impossible. Nous continuons ainsi jusqu'à obtenir un tableau sans coïncidence.

T	B	I	M	Q	W	M	Y	I	C	C	G	N	D
B	U	L	L	E	T	I	N	M	E	T	E	O	N
D	D	U	I	X	W	M	X	N	Z	N	N	R	D
O	R	D	A	T	L	A	N	T	I	Q	U	E	O

Dernière mise en correspondance.

Cette absence de coïncidence nous conduit à essayer nos méthodes sur cette correspondance. Nous y trouvons une paire, ce qui permet d'appliquer la méthode déjà exposée.

T	B	I	M	Q	W		Y		C	C	G	N	D
						M		**I**					
B	U	L	L	E	T		N		E	T	E	O	N
						I		**M**					
D	D	U	I	X	W	M	X	N	Z	N	N	R	D
O	R	D	A	T	L	A	N	T	I	Q	U	E	O

Essai du mot probable.

Erreurs de procédure

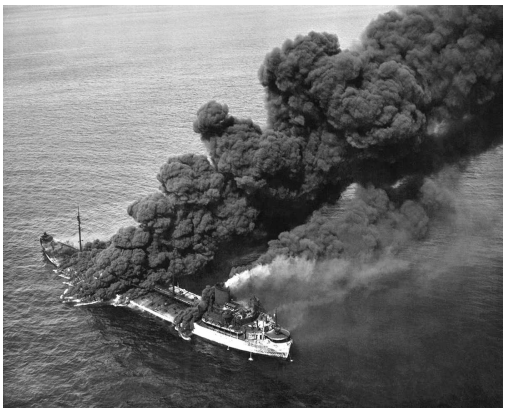
À cause d'un opérateur allemand qui commençait tous ses messages par les initiales C.I.L., les décrypteurs britanniques qualifièrent ce type de messages de « cillies », un terme proche de *silly*, qui signifie « stupide » en anglais. Le début du message pouvait aussi résumer le sujet, comme ceux commençant par « WET » (*Wetter* signifie « temps », dans le sens de celui qu'il fait, en allemand). Ces erreurs n'étaient pas le fait des sous-mariniers, bien plus avertis que leurs collègues de l'armée de terre. Pourtant, ils en pâtirent directement puisque la clef était la même pour tous… Ainsi, elle pouvait être découverte sur un message sans importance et utilisée sur d'autres.

Si les services de renseignements britanniques décryptaient de façon routinière les machines à trois rotors, celles à quatre rotors qu'affectionnait la marine allemande constituaient un tout autre défi. Toutefois, une erreur de procédure allemande incroyable aida les Britanniques. La météo n'étant pas vraiment un secret militaire, la marine allemande envoyait à son quartier général les messages météo chiffrés, mais avec une machine Enigma à trois rotors. Chaque jour, cette Enigma était réglée comme celles à quatre rotors, mais avec le quatrième rotor en moins ! Or ces mêmes bulletins étaient transmis à l'identique aux sous-marins, en étant cette fois bel et bien codés avec des machines à quatre rotors. Les Allemands offraient ainsi des mots probables gigantesques à Turing et son équipe. Les Allemands ne s'aperçurent jamais de cette erreur de procédure. C'est d'ailleurs plutôt étrange : ils se doutaient que les Britanniques savaient décrypter l'Enigma à trois rotors, puisqu'ils étaient passés à quatre !

Gagner la bataille de l'Atlantique

Ce décryptement d'Enigma a influé considérablement sur le déroulement de la guerre, en particulier dans la bataille

sous-marine de l’Atlantique Nord.



Bateau allié coulé par un sous-marin allemand. La victoire alliée dépendait de la quantité d’approvisionnement pouvant atteindre le front.

La tactique des sous-marins était simple : ils quadrillaient l’océan. Le premier qui repérait un convoi prévenait les autres et ensemble les navires prévoyaient une attaque coordonnée. Vu la lenteur des sous-marins, la méthode n’était efficace que si les transmissions restaient absolument secrètes. C’est pourquoi la marine de guerre allemande fut équipée de la version d’Enigma à quatre rotors et au tableau de connexions de dix fiches à partir de février 1942. Ce modèle dominait largement l’Enigma classique à trois rotors et six fiches. Pendant un an, l’équipe de Turing fut incapable de déchiffrer cette nouvelle arme. Les conséquences se voient dans les statistiques de 1941 à 1943 concernant le tonnage coulé par les sous-marins allemands ainsi que le nombre de sous-marins détruits. De février 1942 à avril 1943, les tonnages coulés furent massifs. Ils diminuèrent ensuite grâce notamment au décryptement de l’Enigma version améliorée (et également à l’introduction du sonar).

1941	1	2	3	4	5	6

Tonnage	21	39	41	43	58	61
Sous-marins	0	0	5	2	1	4
	7	8	9	10	11	12
Tonnage	22	23	53	32	13	26
Sous-marins	4	2	2	2	5	10
1942	1	2	3	4	5	6
Tonnage	62	85	95	74	125	144
Sous-marins	3	3	6	3	4	3
	7	8	9	10	11	12
Tonnage	96	108	98	94	119	60
Sous-marins	11	10	10	16	12	6
1943	1	2	3	4	5	6
Tonnage	37	63	108	58	50	20
Sous-marins	7	18	15	16	41	17
	7	8	9	10	11	12
Tonnage	46	16	20	20	14	13
Sous-marins	38	24	11	28	18	10

Tonnage (en milliers de tonnes) et sous-marins coulés selon les mois de la guerre (1 à 12), de 1941 à 1943.

Ce Qu'il Faut Décrypter

Un message de détresse

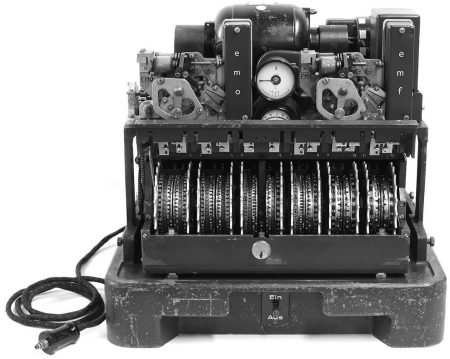
Le message suivant a été chiffré avec une machine Enigma à trois rotors :

FILGA ZMUMY DQNDB CIMHC VAQJY XMNNE JBHNR SMOKF OGXRS JKXYY ZULVI IYPCP JDWBQ TIEOT CACNP VLMTN QQPLD FCULS MYGXW AJNZB RREUP LMXU

Il contient probablement les mots « division », « attaque » et « chars ». Saurez-vous le décrypter ?

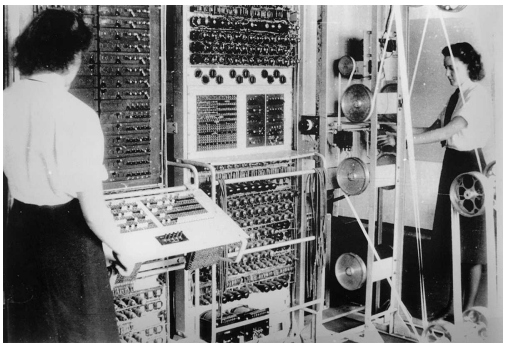
La machine de Lorenz et Colossus

Enigma n'était pas la seule machine à chiffrer allemande. Certaines, estimées plus sûres, comme la machine de Lorenz allemande, étaient réservées aux communications de haut niveau entre le haut commandement et les états-majors des groupes d'armées.



Machine de Lorenz utilisée pour chiffrer les messages entre le haut commandement allemand et ses armées.

Cette dernière fut malgré tout décryptée, encore une fois à cause d'une erreur de procédure. Suite à la demande du destinataire, un même texte avait été envoyé deux fois, avec quelques modifications la seconde : la pire faute que l'on puisse commettre en cryptographie. La machine de Lorenz était fondée sur le masque jetable (en binaire, chaque lettre étant préalablement codée sur cinq bits), mais avec une clef pseudo-aléatoire, c'est-à-dire une clef générée de façon déterministe mais semblant aléatoire. Une erreur de manipulation allemande permit aux Alliés de reconstituer l'algorithme de création des clefs et, en 1943, les Britanniques construisirent Colossus, le premier calculateur électronique de l'Histoire, pour décrypter cette machine.



Dédié à la cryptanalyse, le Colossus Mark 2 britannique contenait 2 400 tubes à vide et pesait 5 tonnes.

Le code pourpre

Tous les belligérants de la guerre disposaient en réalité de machines à chiffrer. Pour leurs relations diplomatiques ou de haut niveau, les Japonais utilisaient une machine dont les Américains avaient baptisé le chiffre « code pourpre », ou de façon moins poétique « code 97 », car son nom japonais faisait référence à l'année 2597 du calendrier japonais (l'année 1937 pour nous). Les Américains décryptèrent le chiffre l'année suivant sa mise en service, en 1938. La veille de l'attaque sur Pearl Harbor, le gouvernement japonais fit parvenir à son ambassade à Washington un document contenant la déclaration de guerre, avec ordre de la remettre au secrétaire d'État américain le lendemain à 13 heures, soit 7 heures 30, heure d'Hawaï. Le service du renseignement décrypta le message et le dimanche 7 décembre à 11 heures 58, soit à 6 heures 28, heure d'Hawaï, le général George Marshall donna l'alerte. Malheureusement, en raison de défaillances techniques, elle arriva à Pearl Harbor plusieurs heures après l'attaque. Ce temps perdu a été à l'origine de polémiques. Certains prétendent que le président Roosevelt aurait laissé faire pour que l'opinion américaine accepte l'entrée en guerre. On peut légitimement douter d'une telle interprétation.

Le décryptement du code pourpre et des autres machines japonaises eut également des conséquences inattendues sur l'espionnage de l'Allemagne. Le général Hiroshi Oshima, ambassadeur à Berlin, et l'amiral Katsuo Abe, attaché naval, furent, sans le vouloir, des sources d'information importantes pour les Alliés, en rapportant consciencieusement à Tokyo tout ce que leur apprenaient les hauts dirigeants allemands sur la conduite de la guerre. Ces renseignements étaient envoyés via le code pourpre… et décryptés par les Américains.

C’est en particulier par cette voie que les Alliés apprirent les caractéristiques des nouveaux sous-marins allemands en juin 1943, leur mode de fabrication par éléments dans des usines souterraines, le transport par voie ferrée sur les lieux d’assemblage, et même les zones prévues pour les essais et l’entraînement des équipages. Ces renseignements permirent aux Alliés de ralentir la mise en service opérationnelle de ces nouveaux sous-marins, en bombardant les points de passage importants et en minant les zones prévues pour l’entraînement.

Les machines françaises

Les Français disposaient bien eux aussi de machines à chiffrer, mais elles se distinguaient de toutes les autres par leur conception. Aux origines de ces machines, on trouve un personnage étonnant, Arvid Damm (1869-1927), un ingénieur suédois initialement spécialiste… des machines à tisser ! Une bizarrerie apparente qui ne doit pas surprendre : ce type de machines avait déjà inspiré Charles Babbage pour sa machine à différence. Damm était le responsable technique d’une fabrique de textile en Finlande et ne manquait pas d’imagination – pour construire des machines comme dans sa vie personnelle (on raconte qu’il organisa un faux mariage pour passer l’alliance au doigt d’une écuyère de cirque, qu’il présenta ensuite comme une espionne à la solde de l’Autriche quand il voulut s’en débarrasser !).

Prenant sans doute conscience du besoin des armées en moyens de chiffrement sûrs et rapides, Damm s’intéressa aux machines à chiffrer dès le début de la Première Guerre mondiale et en fabriqua plusieurs. Pour commercialiser ses inventions, il fonda dès 1915 une entreprise de cryptographie, contrôlée à partir de 1925 par un autre ingénieur, Boris Hagelin. Cette même année, quand l’armée

suédoise voulut s'équiper de machines à chiffrer, Hagelin remporta le marché avec un prototype d'une nouvelle machine, qui deviendra la B-21 utilisée plus tard par les Français.

Comment fonctionnait la B-21 ? La machine produisait un chiffrement de substitution poly-alphabétique, de façon différente de la machine Enigma. Sans entrer trop dans les détails, son originalité était d'utiliser un carré de Polybe pour chiffrer les lettres, ce qui obligeait à supprimer une lettre, W pouvant être remplacé par VV ou omis. Voici un exemple où les abscisses sont notées par les consonnes L, N, R, S et T, et les ordonnées par les voyelles A, E, I, O et U :

	L	N	R	S	T
A	M	U	F	X	Q
E	O	H	V	R	A
I	K	N	Y	D	Z
O	L	I	G	C	E
U	P	J	B	T	S

Ici, le mot « ATTAQUE » devient la suite « ET, US, US, ET, AT, AN, OT », soit la suite de voyelles « EUUEAAO » et celle de consonnes « TSSTTNT ». La décomposition de chaque lettre en une voyelle et une consonne se faisait automatiquement quand on appuyait sur une touche du

clavier. Les voyelles et les consonnes étaient alors chiffrées par deux demi-rotors, l'un étant celui des voyelles et l'autre celui des consonnes. Chacun permettait dix permutations, des voyelles pour le premier et des consonnes pour le second.

Quand on ouvre la B-21, on découvre quatre roues ayant respectivement 17, 19, 21 et 23 positions identifiées par des lettres. Chaque position contient un ergot pouvant être poussé à droite ou à gauche. Leurs positions font partie de la clef. Poussé dans un sens, l'ergot est actif, dans l'autre il est inactif. Ces roues sont destinées à faire avancer les demi-rotors de façon semblant erratique.

Le demi-rotor « voyelle » est contrôlé par les roues à 21 et 23 ergots. Quand on frappe une lettre au clavier, chaque roue progresse d'un cran, faisant ou non avancer le demi-rotor « voyelle » si au moins un des ergots est actif. Il en est de même du demi-rotor « consonne » avec les deux autres roues. Pour compliquer le système, voyelles et consonnes sont également permutées grâce à un tableau de fiches qui, à la différence des demi-rotors, assurent la même permutation tout au long du chiffrement. Sur le côté de la B-21, on trouve une petite manette pouvant prendre deux positions : chiffrement et déchiffrement.

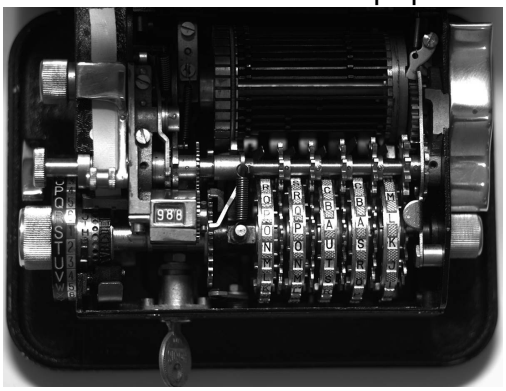
La B-21, son clavier à 25 touches (le W manque) et ses 25 lampes. Quand on frappe une lettre sur le clavier, la lettre chiffrée s'illumine, comme sur l'Enigma.

L’armée française s’y intéressa et demanda des améliorations, notamment la possibilité d’imprimer les messages. Le résultat fut la B-211. Cinq cents exemplaires furent livrés en 1939. Cette machine fut aussi utilisée par les Pays-Bas … et l’Union soviétique qui, après en avoir acheté un exemplaire en Suède, par autorisation du gouvernement suédois, la copia et la nomma K-37 Crystal. En 1942, la B-211 fut ensuite équipée d’un élément appelé surchiffreur qui la rendait inviolable à l’époque. Durant la guerre, les Allemands réussirent à casser la B-211, mais sans son surchiffreur.

La C-36

La B-211 était réservée au niveau stratégique, elle tenait dans un attaché-case plutôt lourd. L’armée française voulut commander une machine légère pour le niveau tactique, de la taille d’une boîte à sucre et purement mécanique. Hagelin réussit le tour de force de fabriquer un tel engin. Ce fut la C-36, dont l’armée acheta 5 000 exemplaires, livrés avant le début de la guerre. La C-36 a été ensuite perfectionnée, devenant la M-209 de l’armée américaine. Cette machine était assez sûre pour son niveau d’utilisation. Cependant, dès 1943, les Allemands étaient capables de décrypter ses messages en quelques heures.

C-36 fermée. Les cinq lettres visibles sur le capot (ici MNTRJ) constituent une clef modifiable à chaque message. La machine est actionnée par le levier de droite. Les lettres à chiffrer sont choisies sur la roue de gauche et le chiffrement sort sur la bande de papier à gauche.



C-36 ouverte. Les ergots des rotors sont visibles, chacun étant poussé vers la droite ou la gauche, ce qui constitue la clef principale avec la position d'un élément (case grisée) sur la roue de gauche (ici devant le S).

Le mécanisme de la C-36 repose sur un ensemble d'engrenages, entraînés par une série de cinq rotors ayant respectivement 17, 19, 21, 23 et 25 ergots, qui doivent être configurés manuellement chaque jour selon un tableau tenu secret. Avec la position de la roue de gauche (celle

comportant une marque), l'ensemble constitue la clef du jour. Une seconde clef, choisie par l'opérateur à chaque message, est déterminée par la position initiale des rotors, visible quand le capot est fermé. Elle est envoyée en clair, mais de façon camouflée, dans le style de l'alphabet radio où « bravo » signifie « B ».

Après le chiffrement d'une lettre du message, chaque roue avance d'un cran et une nouvelle configuration d'ergots est mise en place pour chiffrer la lettre suivante. Le message est chiffré ainsi lettre par lettre et le résultat imprimé sur une bande de papier. Il est déchiffrable à l'aide d'une autre C-36 réglée de la même manière. La C-36 a eu plusieurs successeurs dans l'armée française, parmi lesquels la CX-52 entrée en service en 1952, dont on voit tout de suite la similarité avec la C-36. Cette machine s'est maintenue jusqu'aux années 1980.

La machine à chiffrer CX-52 de Hagelin. On remarque le H du logo en haut.

L'armée française a utilisé une autre machine de ce type, compatible avec la CX-52, mais pouvant rentrer réellement dans une poche : la CD-57. Elle fut à l'œuvre jusqu'au milieu des années 1970.

Lors de la crise de Suez de 1956, les Britanniques firent savoir aux Français qu'il ne fallait plus recourir à la B-211,

alors toujours en service. Cet avertissement provoqua la recherche d'une machine à chiffrer plus sûre. On se tourna alors vers une machine de l'OTAN, construite sur les principes de l'Enigma mais à huit rotors, la KL-7. On revint aussi au masque jetable, comme dans la machine de Lorenz, mais avec des clefs réellement aléatoires, qui devaient être additionnées bit à bit au message pour obtenir le message chiffré. Ce fut la machine TAREC (pour « transmission automatique régénératrice et chiffrante »), utilisée par l'OTAN dès le milieu des années 1950. La méthode avait l'avantage de permettre des communications sécurisées, mais présentait comme inconvénient la lourdeur de la distribution des clefs et l'obligation de respecter la procédure de destruction des clefs après un usage unique.

Le problème principal était que suivre cette procédure demandait soit une formation mathématique de bon niveau, soit une obéissance de niveau supérieur ! André Muller, chef du service qui fabriquait les clefs aléatoires, raconte qu'en 1968, un général responsable des transmissions d'une des armées décida de les employer deux fois, pensant que la règle de ne les utiliser qu'une fois était une invention du service fabriquant les clefs pour gagner plus d'argent. Il fallut l'intervention des plus hautes autorités du Chiffre pour faire revenir le haut gradé sur sa décision !

La France développa ensuite une machine électronique de chiffrement, à base de transistors au germanium, fondée comme la machine de Lorenz sur le masque jetable, avec une clef pseudo-aléatoire : la machine Myosotis. La clef était produite à la volée, bit après bit. Conçue dans les années 1960, la Myosotis restera en service pendant plus de vingt ans. Elle fut l'une des meilleures machines de son époque.

Le chiffrement de la voix

Parallèlement à la conception de toutes ces machines, fondées sur des lettres et des nombres, d'autres systèmes cherchèrent à coder directement la voix. Après l'attaque-surprise de la marine japonaise sur Pearl Harbor le 7 décembre 1941, le développement d'un système de communication vocale sécurisé fut considéré comme une priorité par les États-Unis. Claude Shannon participa à ce projet et peut-être aussi Alan Turing pour les tests, puisqu'il séjourna aux États-Unis en 1943. La réponse fut le système Sigsaly, déployé courant 1943. Ce nom ressemble à un acronyme, mais il s'agit d'un simple code ; le début Sig est juste commun à la machine chiffrante Sigaba.

Le principe de chiffrement est l'addition à la voix d'un bruit aléatoire stocké sur des disques de phonographe. Ce bruit doit être soustrait à la réception. Ces disques constituent la clef qui doit être partagée. Vous reconnaîtrez le principe du masque jetable appliqué au son.

Le système fut en service de 1943 à 1946, où 12 terminaux furent installés de par le monde. Avec succès puisque les puissances de l'Axe ne furent jamais capables de décrypter une seule des 3 000 conférences tenues via Sigsaly. Chaque terminal pesait 55 tonnes, occupait plus de 200 m² au sol, demandait 13 techniciens en permanence et devait être climatisé. Dans les années 1960, le chiffrement s'était miniaturisé mais restait très lourd. Ces inconvénients disparurent avec l'entrée dans l'ère numérique.

12
L'ère numérique et la cryptographie quantique

Ouvrir sa voiture avec un bipeur, allumer son téléphone portable, se connecter à un réseau Wi-Fi, consulter son compte bancaire en ligne, etc. : autant d'opérations qui mettent en œuvre des codes secrets, sans qu'on le sache toujours. Il faut s'y résoudre : la cryptographie a envahi notre quotidien. Il est loin le temps où les cryptologues de la Première Guerre mondiale travaillaient sur des coins de table pour décoder les messages ennemis. Le moteur de cette ubiquité ? L'ordinateur bien sûr, qui a accéléré la demande de sécurisation des communications de façon exponentielle, et l'a sortie du pré carré des militaires et des diplomates.

C'est quoi, les nombres binaires ?

Afin de pouvoir comprendre comment l'ère numérique a complètement rebattu les cartes de la cryptographie, il faut que vous puissiez parler le B.A.-BA de la langue des ordinateurs, à savoir le langage binaire. Rien là-dedans de fondamentalement nouveau par rapport au système que nous employons tous les jours : le binaire est à 2 ce que le décimal est à 10.

De la même manière que, dans la vie quotidienne, nous décomposons chaque nombre en puissances de 10 (125 = 100 + 2 × 10 + 5 × 1), le langage binaire écrit les nombres avec des puissances de 2. C'est ainsi que le nombre 2 s'écrit 10 en binaire : 1 × 2 + 0 × 1. Quant au nombre 3, c'est 11 : 1 × 2 + 1 × 1 tandis que 13 s'écrit 1101 : 1 × 8 + 1 × 4 + 0 × 2 + 1 × 1. De cette façon, tous les nombres décimaux entre 0 et 255 s'écrivent avec huit bits (c'est-à-dire huit chiffres binaires) au plus.

Ce préambule établi, regardons comment coder n'importe quelle lettre d'un message en langage binaire. Pour manipuler des lettres et non plus des nombres, il suffit de les transformer d'abord au moyen du code ASCII, qui fait correspondre les caractères alphanumériques (lettres, chiffres, signes de ponctuation, etc.) à des nombres entre 0 et 255. Ainsi, « attaque » devient en caractère ASCII la suite de nombres :

97 116 116 97 113 117 101

ce qui fait penser aux anciennes tables de chiffrement, au Grand Chiffre de Louis XIV en particulier. En codant chaque nombre de cette suite sur sept bits nous obtenons :

1100001 1110100 1110100 1100001 1110001 1110101 1100101

Même si les espaces n'ont aucun intérêt quand ces nombres sont transmis par des ordinateurs, nous continuerons à les ajouter pour faciliter la lecture.

33	!	49	1	65	**A**	81	**Q**	97	a	113	q
34	"	50	2	66	**B**	82	**R**	98	b	114	r
35	**#**	51	3	67	**C**	83	**S**	99	c	115	s

36	$	52	4	68	**D**	84	**T**	100	d	116	t
37	%	53	5	69	**E**	85	**U**	101	e	117	u
38	&	54	6	70	**F**	86	**V**	102	f	118	v
39	‘	55	7	71	**G**	87	**W**	103	g	119	w
40	(	56	8	72	**H**	88	**X**	104	h	120	x
41	)	57	9	73	**I**	89	**Y**	105	i	121	y
42	*	58	:	74	**J**	90	**Z**	106	j	122	z
43	+	59	;	75	**K**	91	[	107	k	123	{
44	,	60	<	76	**L**	92	\	108	l	124	|
45	-	61	=	77	**M**	93	]	109	m	125	}
46	.	62	>	78	**N**	94	^	110	n	126	~

47	/	63	?	79	**O**	95	_	111	o
48	0	64	@	80	**P**	96	`	112	p

Table du code ASCII (*American Standard Code for Information Interchange*, ou « Code américain normalisé pour l'échange d'information »).

Vigenère en binaire

L'avantage du langage binaire ? Il simplifie considérablement les opérations. Le chiffrement de Vigenère (p. 205), par exemple, est facilité puisque l'alphabet est réduit à deux symboles, au lieu des 26 habituels : 0 et 1. L'ajout de 0 à une « lettre » (0 ou 1) ne la modifie pas, l'ajout de 1 la change en l'autre lettre. Cela revient à chiffrer le message en ajoutant (sans retenue) au message la clef bit à bit. Imaginons que nous cherchions à transmettre le message « demain, quatre heures, attaque en direction d'Amiens ». Sa version ASCII est :

10001 00110 01011 10110 11100 00111 01001 11011 10010 11000 10000
01110 00111 10101 11000 01111 01001 11001 01100 10101 00000 11010
00110 01011 11010 11110 01011 00101 11100 11010 11000 10000 01100
00111 10100 11101 00110 00011 11000 11110 10111 00101 01000 00110
01011 10111 00100 00011 00100 11010 01111 00101 10010 11100 01111
10100 11010 01110 11111 10111 00100 00011 00100 01001 11100 00011
10110 11101 00111 00101 11011 10111 00110 10111 0

Comme clef, nous utilisons une suite aléatoire de 0 et de 1 de même longueur, par exemple :

10010 10110 00011 10110 00001 01010 11001 01101 01000 00000 00100
01000 00100 10110 00100 00111 01110 01101 01111 00111 01001 10010
11100 00010 00000 11010 11101 11100 10110 00000 00101 01101 11011
10111 11111 10010 11101 00010 10111 01110 11100 00111 01010 11110
00001 01101 01000 01010 10010 01110 11001 11110 01010 00100 01100
10110 01101 10101 11110 01000 11000 01101 01101 10011 00000 00100
01000 01010 01000 01111 10001 11110 11111 11111 1

En principe, une telle clef peut provenir de lancers consécutifs d'une pièce de monnaie. En pratique, on ne procède pas ainsi, car la production de clefs serait trop longue. Voici le résultat du chiffrement du premier terme du message :

Message	1	0	0	0	1
Clef	1	0	0	1	0
Message chiffré	0	0	0	1	1

Chiffrement d'un message.

À chaque étape, nous avons effectué l'addition de deux bits, ceux qui se correspondent dans le message et la clef. La seule surprise vient quand on ajoute 1 et 1, puisque cela donne 0. Autrement dit, la table d'addition n'est pas la table usuelle.

+	0	1
0	0	1
1	1	0

Pour déchiffrer, il suffit d'ajouter la clef au message chiffré pour obtenir le message en clair ! Pourquoi ? Tout simplement parce que chacun des deux bits vérifie la même relation : 0 + 0 = 0 et 1 + 1 = 0. Le tableau *Déchiffrement* montre ce que cela donne pour les premiers bits de notre exemple.

Message	1	0	0	0	1
Clef	1	0	0	1	0
Message chiffré	0	0	0	1	1
Clef	1	0	0	1	0
Message déchiffré	1	0	0	0	1

Déchiffrement d'un message en réutilisant la clef.

Nous obtenons ainsi le message chiffré :

00011 10000 01000 00000 11101 01101 10000 10110 11010 11000 10100
00110 00011 00011 11100 01000 00111 10100 00011 10010 01001 01000
11010 01001 11010 00100 10110 11001 01010 11010 11101 11101 10111
10000 01011 01111 11011 00001 01111 10000 01011 00010 00010 11000
01010 11010 01100 01001 10110 10100 10110 11011 11000 11000 00011
00010 10111 11011 00001 11111 11100 01110 01001 11010 11100 00111
11110 11111 01111 01010 01010 01001 11001 01000 1

L'ensemble de ces opérations revient à utiliser un masque jetable, comme celui exploité par le téléphone rouge. Ce masque jetable, que Claude Shannon a montré inviolable sous la condition que la clef soit aléatoire et d'un usage unique, avait toutefois un inconvénient fondamental selon le grand cryptologue Horst Feistel (1915-1990), que nous retrouverons plus loin à propos du chiffre DES :

> Pour chaque bit d'information transmise, le destinataire doit avoir en sa possession à l'avance un bit d'information de clef. De plus, ces bits doivent être une suite aléatoire qui ne peut pas être utilisée une seconde fois. Pour un gros volume de trafic, il s'agit là d'une restriction sévère. Pour cette raison, le système de Vernam est réservé aux messages top-secrets.

De l'usage des suites pseudo-aléatoires

La sécurité du chiffre de Vernam (p. 239) dépend du côté aléatoire de la clef, mais comment fabriquer de l'aléatoire ? *A priori*, il faudrait recourir à un phénomène réellement lié au hasard, comme le jet d'une pièce de monnaie : or c'est impraticable. Une autre idée est de se contenter d'une suite dont un terme n'est pas prévisible en fonction des précédents. Dans la pratique, on emploie des suites qui n'ont pas de règle de construction simple. Je vous propose d'en détailler une qui fut autrefois à l'œuvre et qui reste typique d'un grand nombre de suites « pseudo-aléatoires ».

L'idée est de partir d'un nombre, que l'on nomme traditionnellement le germe. On multiplie ce nombre par 16 807, puis l'on prend le reste du résultat dans la division par 2 147 483 647. Cela fournit une suite de nombres compris entre 0 et 2 147 483 646 qui comporte de nombreux aspects du hasard. Par exemple, si nous prenons 21 comme germe, nous obtenons la suite : 21, 352 947, 1 637 012 935, 1 863 396 828, 1 356 463 995, etc. Nous pouvons convertir ces nombres en binaire et les accoler les uns aux autres :

10101 10101 10001 01011 00111 10000 11001 00101 10101 01110 00111 11011 11000 10001 00101 10111 01110 01010 00011 01100 11111 11110 11110 11

Une telle suite ressemble à une suite aléatoire. Pourtant, si nous connaissons la règle, elle est prévisible dès que l'on connaît son premier terme.

À l'assaut d'un « masque jetable pseudo-aléatoire »

Ce germe peut être découvert grâce à la méthode du mot probable. Considérons le message suivant, chiffré avec la suite pseudo-aléatoire précédente :

00001 11110 00111 11011 00011 11011 11111 10010 00100 01010 11111 00010 01001 11100 00001 10101 01010 11011 01100 01100 00001 01100

11110 11011 10110 10110 11110 11110 10101 11110 01100 10110 11001 11110 11101 11111 00100 1111

Nous ignorons seulement le germe utilisé, mais pensons que le message doit commencer par le mot « Attaque », c'est-à-dire par :

10000 01111 01001 11010 01100 00111 10001 11101 01110 0101

Si tel est le cas, en ajoutant cette suite de bits au message, nous obtenons le début de la clef. Cette addition donne :

10001 10001 01110 00001 01111 11100 01110 01111 01010 0000

Le germe utilisé peut se trouver là. Bien entendu, plusieurs essais sont nécessaires pour le repérer. Quelques tâtonnements amènent à essayer « 10001 » en binaire, soit 17. Le deuxième terme est alors 285 719, soit « 10001 01110 00001 0111 », ce qui correspond parfaitement. Le suivant est « 507 111 939 ». La clef devient :

10001 10001 01110 00001 01111 11100 01110 01111 01010 00000 011

La correspondance est parfaite. Nous continuons donc la suite pseudo-aléatoire par « 1 815 247 477, 1 711 656 657, 122 498 987, 1 551 140 683, 1 717 468 248 », ce qui fournit la clef :

10001 10001 01110 00001 01111 11100 01110 01111 01010 00000 01111 01100 00110 01001 11101 00111 01011 10011 00000 01011 10011 10110 10001 11101 00110 10010 11111 01010 11101 11000 11101 00100 00111 01001 01111 00110 01011 11001 11110 00101 10

En l'additionnant au message chiffré, nous obtenons :

10000 01111 01001 11010 01100 00111 10001 11101 01110 01010 10000 01110 01111 10101 11100 10010 00001 01000 01100 00111 10010 11010 01111 00110 10000 00100 00001 10100 01000 00110 10001 10010 11110 10111 10010 11001 01111 0011

ce qui signifie « Attaque sur Paris 4 heures ». La connaissance du système de chiffrement a suffi pour que nous décryptions le message. L'une des faiblesses du masque jetable se situe là : il est indécryptable… tant qu'on respecte l'hypothèse de départ.

Nos services de renseignements ont appris que l'adversaire privilégiait un masque jetable et générait sa clef de la façon suivante : il prend l'heure en seconde comme germe puis multiplie le nombre obtenu par 425 612, ajoute 91 787 et garde le reste dans la division par 2 265 536 135. Il recommence ainsi aussi longtemps que nécessaire pour obtenir une clef binaire de la longueur du message. Celui-ci est d'abord codé en ASCII sur sept bits. Nous avons intercepté le message suivant :

00110 11110 01010 01010 01110 11101 11000 10111 10111 10111
00010 10111 00000 10000 01010 11010 10000 00100 11111 00000
11110 10000 01011 00100 00010 00110 01011 01001 10010 10111
11010 11010 10110 00001 00110 10101 11011 01010 11001 00000
01001 01010 00100 01001 10101 10001 10111 01110 01000 00101
01100 10110 01000 01101 01000 01010 01000 10011 10010 01111
00100 11101 11011 00001 11111 00111 00000 01001 11000 00001
11110 00011 10011 10110 00100 10011 11011 01000 10011 01100
00111 10101 11001 10110 10011 00001 00101 11110 10111 10110
00000 11000 11110 00010 10001 01001 01100 01100 11100 10110
01111 11011 00100 101

Nous pensons qu'il commence par « Du Haut Quartier Général ». Saurez-vous le décrypter ?

Le Wi-Fi et les portables

Le mot « Wi-Fi » a été choisi par ses concepteurs pour sonner comme « Hi-Fi » et n'a pris qu'ensuite le sens de *wireless fidelity*. Sa sécurité est souvent assurée par une clef dite WEP (*Wired Equivalent Privacy*). Ce mot signifie que la confidentialité obtenue est équivalente à celle d'un réseau filaire… ce qui est faux, bien sûr. Vous devez rentrer laborieusement cette clef WEP dans votre ordinateur. Il s'agit d'une suite de 128 bits, mais le système vous demande d'introduire 26 chiffres hexadécimaux (les chiffres du système de base 16), comme

9A8356D713058F4569C54039A0. Chaque chiffre correspond donc à quatre bits selon la table proposée ci-dessous.

0	1	2	3	4	5	6	7
0000	0001	0010	0011	0100	0101	0110	0111
8	9	**A**	**B**	**C**	**D**	**E**	**F**
1000	1001	1010	1011	1100	1101	1110	1111

Signification des chiffres hexadécimaux, c'est-à-dire des chiffres du système de base 16. En plus des chiffres usuels, ce système utilise les chiffres A, B, C, D, E et F qui représentent 10, 11, 12, 13, 14 et 15.

Notre clef correspond donc ici à :

1001 1010 1000 0011 0101 0110 1101 0111 0001 0011 0000 0101 1000 1111 0100 0101 0110 1001 1100 0101 0100 0000 0011 1001 1010 0000

puisque chaque chiffre hexadécimal représente quatre bits. La clef de 26 chiffres représente donc 26 × 4, soit 104 bits. Les 24 autres sont ajoutés par le système. Cet ajout sert au moment de l'initialisation et évite que la clef soit toujours la même. Cette clef va de pair avec un algorithme de chiffrement nommé RC4, créé par un cryptologue américain que nous rencontrerons quand nous étudierons le système RSA, car il s'agit de l'un de ses inventeurs : Ronald Rivest.

RC signifie *Rivest Cypher* (« chiffre de Rivest »). RC4 est un masque jetable pseudo-aléatoire comme celui que nous venons de voir. Avec le matériel adéquat, il est cassable en deux minutes environ. Il n'offre donc qu'une sécurité illusoire… RC4 est également utilisé par le système WPA, un des autres systèmes de cryptographie sur lesquels s'appuie le Wi-Fi. Si vous désirez appliquer un algorithme encore sûr

à l'heure actuelle, il faut vous tourner vers le système WPA-2, dont le cœur est l'algorithme AES qui sera évoqué plus loin.

Les communications des téléphones portables GSM (*Global System for Mobile Communications*) sont chiffrées de façon comparable par un algorithme portant le nom d'A5/1. Pour chaque appel, une clef de 64 bits est envoyée. Combinée à la clef contenue dans la carte SIM du téléphone, elle sert de germe à une suite de nombres pseudo-aléatoires de 228 bits chacun, dont les détails peuvent être connus mais sont théoriquement secrets, si bien que nous ne la donnerons pas ici ! Celui qui veut se la procurer n'aura aucun mal puisqu'on la trouve sur Internet.

De nos jours, une communication peut être décryptée en temps réel dès lors qu'elle dure au moins deux minutes. Pour cela, il faut cependant disposer des informations et de l'équipement nécessaires… et réussir à capter la conversation. Il est malgré tout fort probable que l'algorithme de chiffrement soit modifié d'ici quelques années, du moins nous l'espérons.

Des suites vraiment aléatoires ?

Le défaut des suites pseudo-aléatoires est d'être fondées sur des processus déterministes. Pour éviter le type de décryptement que nous venons d'examiner, il est nécessaire d'injecter le maximum de vrai hasard dans la construction de la suite, pas seulement dans le germe. Pour ce faire, on peut tenter l'heure en secondes, le temps d'accès au disque dur, le bruit créé par un micro enregistrant le vent, etc. À chaque étape de la suite, nous introduisons donc un aléa de ce type. On comprend qu'il devient alors très difficile de déterminer la clef !

Une autre faiblesse du masque jetable est le transfert de cette clef. Certes, les ambassades utilisent la valise

diplomatique pour transmettre leurs informations confidentielles, tandis qu'il arrive aux armées et même à certaines entreprises de recourir ponctuellement à des procédés comparables. En revanche, la méthode est impraticable pour des opérations à grande échelle ou routinières. Pour le commerce par Internet, par exemple, qui exige des millions de communications par seconde, on fait appel à d'autres types de chiffrement (voir le chapitre 13). Cependant, une nouvelle technique, la cryptographie quantique, assure le transfert sécurisé de clefs, même s'il est encore limité en distance.

Merveilles quantiques

La cryptographie quantique se fonde sur les propriétés à la fois étranges et fascinantes de la physique quantique. Étranges car, dans cette discipline, l'observation modifie l'objet observé ! Imaginons que nous codions un message à l'aide de particules élémentaires de lumière, des photons. Chaque photon peut être polarisé, c'est-à-dire que l'on peut imposer une direction à son champ électrique. Cette polarisation peut être aléatoire, comme dans le cas d'une ampoule à filament, mais aussi imposée. Vous voyez qu'en faisant basculer la polarisation entre deux directions, il devient possible de transmettre des messages binaires ! Or d'après la physique quantique, dès qu'on intervient sur un système, on l'altère. En l'occurrence, si jamais un espion intercepte certains des photons, la polarisation de ceux-ci sera modifiée et nous le découvrirons à la réception. La cryptographie quantique incarne un peu le Graal de tout cryptologue : on sait immédiatement si le message a été écouté !

En 1984, deux chercheurs canadiens, Charles Bennett et Gilles Brassard, mirent en œuvre cette idée avec des photons polarisés à 0°, 45°, 90° ou 135°. Les deux

premières polarisations représentent le bit 0, les autres l, ou vice versa. Les interlocuteurs (émetteur et récepteur) disposent de deux liaisons : une fibre optique et une liaison radio. Par la fibre, l'émetteur envoie une suite de photons polarisés aléatoirement. Le récepteur les fait passer à travers un filtre polarisant, orienté aléatoirement à 0° (rectiligne) ou 45° (diagonal) derrière lequel est situé un détecteur de photons. Si le filtre est rectiligne, un photon orienté à 0° le traverse puis est détecté. Un photon orienté à 90° est arrêté. En revanche, un photon orienté à 45° ou 135° traverse le filtre avec une probabilité de 0,5.

Ainsi, on peut distinguer entre un photon à 0 ou 90°, mais pas entre des photons à 45° ou 135°. De même, un filtre diagonal discrimine les photons à 45° de ceux à 135°, mais pas ceux à 0° de ceux à 90°. Le récepteur note 0 si le photon traverse et 1 sinon. Pour éliminer les cas d'incertitude, il donne l'orientation de son filtre à la réception (diagonal ou rectiligne). Si elle diffère de celle à l'émission, le bit envoyé est incertain donc supprimé. La clef transmise est la suite des bits conservés.

Émission	0°	45°	90°	45°	0°	135°	90°	0°
Bit envoyé	0	0	1	0	0	1	1	0
Filtre réception	diag	diag	rect	diag	rect	rect	rect	diag
Traverse ?	non	oui	non	oui	oui	non	non	non
Bit reçu	1	0	1	0	0	1	1	1
Clef		0	1	0	0		1	
	X					**X**		**X**

Suite d'émission de photons, réception et clef obtenue.

En cas d'interception de la communication, un espion doit émettre les photons correctement vers le récepteur. Pour

cela, il doit procéder comme le récepteur, puis réémettre. Puisqu'il a une chance sur deux d'avoir choisi le mauvais filtre, la moitié de ses photons réémis seront faux. La méthode autorise une transmission sûre des clefs du chiffre de Vernam ou de tout autre système cryptographique. Elle assure également la création de clefs véritablement aléatoires.

La cryptographie quantique est devenue une réalité depuis cette première traduction expérimentale. Elle a aujourd'hui quitté le domaine de la recherche fondamentale pour atteindre celui du développement et de la commercialisation. Cependant, vitesse et distance de transfert restent limitées : un millier de bits par seconde, pour une distance maximale de 300 kilomètres. En 2017, les Chinois ont même réussi à échanger entre la Terre et un satellite à une distance de 1 200 kilomètres ! Les difficultés restent nombreuses et, comme toujours dans le domaine du secret, il est difficile de connaître tous les résultats des recherches menées…

Les subtilités du chiffre DES

Le chiffrement de type masque jetable vu précédemment fonctionne par flot continu. Pour être sûr, il exige une clef aléatoire aussi longue que le message, ce qui peut être illusoire. Une méthode plus solide consiste à découper le message par blocs, de 64 bits en général, et de traiter chaque bloc indépendamment. Elle correspond à une adaptation du surchiffrement déjà rencontré à l'époque de la Première Guerre mondiale.

L'idée générale est relativement classique. On effectue d'abord une permutation sur le bloc, puis des substitutions de type Vigenère mélangées avec d'autres permutations… et on recommence un plus ou moins grand nombre de fois suivant les méthodes. Elles sont nombreuses, quoique

toutes de natures comparables. Nous nous contenterons donc d'en étudier une : le chiffre DES.

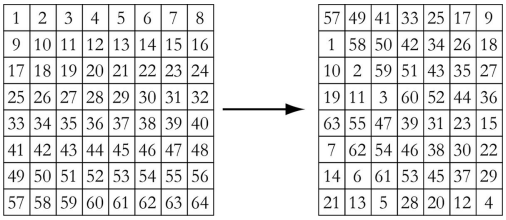
Quand, en mai 1973, le National Bureau of Standards lança un appel d'offres pour un système de chiffrement, IBM proposa son chiffre nommé Lucifer, un procédé d'une complexité infernale créé par Horst Feistel et que seul un ordinateur pouvait manipuler. Pour cette raison sans doute, il remporta le concours et fut modifié pour devenir le code DES (*Data Encryption Standard*, « standard de codage des données »). Ce chiffre scinde d'abord le message en blocs de 64 bits, pour les chiffrer grâce à une clef de 64 bits également, manipulée de façon subtile.

Codes détecteurs d'erreurs

À l'ère numérique, les messages transmis sont de longues suites de bits. Comment vérifier qu'ils arrivent intacts ? La méthode classique est d'ajouter des bits de parité à chaque groupe de 7, de sorte que la somme des 8 bits ainsi formés soit paire. Si une seule erreur de transmission est commise sur ces 8 bits, elle sera automatiquement détectée. Il faudra alors reprendre la transmission de ce groupe défectueux.
Ainsi, à 0110101, on ajoutera 0 pour former 01101010. Si un seul bit est modifié, nous savons qu'une erreur s'est produite. Par exemple, 01100111 contient une erreur puisque sa somme est 5, qui est impair. Un tel code est appelé code détecteur d'erreurs. Il existe également des codes permettant de corriger automatiquement les erreurs.

Génération des clefs

Les 64 bits de la clef contiennent 8 bits dits de contrôle, pour éviter les erreurs de transmission (voir l'encadré ci-dessus). Ces bits supplémentaires occupent les positions 8, 16, 24, etc., et ont la parité de la somme des 7 bits qui les précèdent. Par exemple, si les 7 premiers bits de la clef secrète sont 0011010, le 8^{e} est 1 pour qu'il y ait un nombre pair de 1. Cette clef de 64 bits génère 16 clefs de 48 bits utilisées dans les phases de l'algorithme appelées « rondes ». Pour créer ces 16 clefs, les bits de contrôle sont supprimés et les autres permutés (voir la figure ci-dessous) selon un procédé adapté à l'application sur ordinateur. Nous le montrons ici, surtout pour insister sur ce fait : cette méthode est totalement inadaptée à l'utilisation par un être humain, même obsédé par les chiffres. N'essayez donc pas de le faire. Je donne ces détails pour montrer le type de calculs effectués : des substitutions et des transpositions, comme en 1914… mais plus du tout exécutables à la main !



Première permutation de la clef. Les bits de contrôle, dont les positions sont multiples de 8, sont supprimés.

Par exemple, si notre clef de départ est :

00010010 11000101 01010110 01111000 10011010 10111101 11011110 11110000

où nous avons groupé les bits par 8 afin de correspondre au tableau précédent, la meilleure procédure pour effectuer la permutation à la main est de remplir un tableau dont la première ligne est constituée des nombres de 1 à 64, la deuxième des bits de la clef de départ et la ligne suivante

des bits réordonnés selon le tableau de la permutation. Après un calcul pénible, la première permutation donne :
1111001 0110011 1010101 0001111 0101010 1011001 1001111 0001101.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
0	0	0	1	0	0	1	0	1	1	0	0	0	1	0	1
1	1	1	1	0	0	1	0	1	1	0	0	1	1	1	0

17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
0	1	0	1	0	1	1	0	0	1	1	1	1	0	0	0
1	0	1	0	1	0	0	0	1	1	1	1	0	1	0	1

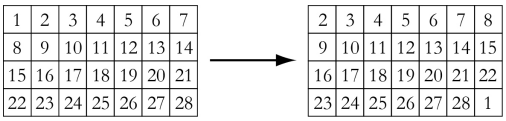
33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
1	0	0	1	1	0	1	0	1	0	1	1	1	1	0	1
0	1	0	1	0	1	1	0	0	1	1	0	0	1	1	1

49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64
1	1	0	1	1	1	1	0	1	1	1	1	0	0	0	0
1	0	0	0	1	1	0	1								

Transformation de la clef par la première permutation. En première ligne, nous lisons les numéros des bits, en deuxième, les bits de notre exemple et en troisième ligne, le bit permuté. En première position, nous trouvons donc le bit en position 57, etc.

Les bits sont alors répartis en partie gauche et partie droite, ici : 1111001 0110011 1010101 0001111 et 0101010 1011001 1001111 0001101

qui subissent chacune un décalage d’un cran vers la gauche aux étapes 1, 2, 9, 16 et de deux crans aux autres étapes.



1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28

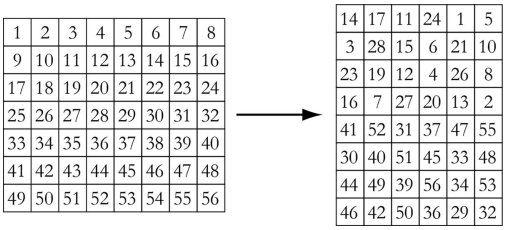
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	1

Décalage d'un cran vers la gauche d'un bloc de 28 bits.

Nous obtenons donc :

1110010 1100111 0101010 0011111 et 1010101 0110011 0011110 0011010

Ces deux blocs sont ensuite regroupés pour former un bloc de 56 bits, ici : 1110010 1100111 0101010 0011111 1010101 0110011 0011110 0011010, qui subit une permutation pour former la clef de 48 bits annoncée.



1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

Deuxième permutation de la clef.

De même, un calcul en tableau permet d'effectuer cette permutation.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	1	1	0	0	1	0	1	1	0	0	1	1	1	0	1
1	0	0	1	1	0	1	1	0	1	0	0	0	0	1	0

17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
0	1	0	1	0	0	0	1	1	1	1	1	1	0	1	0
1	1	1	0	1	1	1	1	1	1	1	1	1	1	0	0

33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48

1	0	1	0	1	1	0	0	1	1	0	0	1	1	1	1
0	1	1	1	0	0	0	0	0	1	1	1	0	0	1	0

49	50	51	52	53	54	55	56
0	0	0	1	1	0	1	0

Transformation de la clef par la deuxième permutation. En première position, nous trouvons donc le bit en position 14, etc.

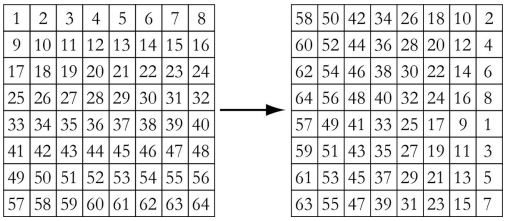
Cet algorithme est itéré seize fois pour fournir les 16 clefs nécessaires aux rondes.

Clef 1	100110 110100 001011 101111 111111 000111 000001 110010
Clef 2	011111 011000 111011 011011 110110 111100 100110 100101
Clef 3	011101 111111 100010 001010 010000 100100 111110 011001
Clef 4	001110 101010 110111 010110 110110 110011 000100 011101
Clef 5	011111 000110 110000 011111 111000 110101 001110 101000
Clef 6	011001 111010 010100 111100 010100 000011 101100 101111
Clef 7	110011 101000 110010 110111 111101 100001 100010 111100
Clef 8	111111 111010 101000 111010 010000 010011 101111 111011
Clef 9	111000 011101 101110 101111 111011 001110 011110 000001
Clef 10	101100 011011 001111 000111 101110 100100 011001 001111
Clef 11	001100 010101 111011 110011 110111 101101 001110 000010
Clef 12	111101 010111 000111 110100 100101 000110 011101 101001
Clef 13	100101 101100 011111 010101 111110 101011 101001 000000
Clef 14	010111 110101 001100 110111 111100 001110 011100 111010
Clef 15	101011 111001 000111 101101 001111 010011 111000 001010
Clef 16	110010 111011 010110 011011 000010 100001 011111 110101

Les clefs pour les 16 rondes.

Permutation initiale

À partir de ces 16 clefs, l'algorithme DES opère sur des blocs de 64 bits, que nous représentons dans un carré de côté 8 pour simplifier. Le bloc subit d'abord une permutation que l'on peut visualiser géométriquement comme précédemment. Encore une fois, pour un être humain, elle serait compliquée, voire impossible à réaliser.



1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

Permutation initiale. Le bit en position 58 du carré initial est placé en première position, celui en position 50 à la deuxième, etc.

En guise d'exemple, considérons le message « attaques ». En ASCII sur 8 bits, cela donne un bloc de 64 bits, que nous groupons par huit pour faciliter la lecture :

01100001 01110100 01110100 01100001 01110001 01110101 01100101 01110011

Ce bloc est transformé par la permutation initiale en un autre bloc de 64 bits. À la main, ce travail est aussi fastidieux que sujet à erreurs. On comprend pourquoi de telles méthodes étaient inapplicables avant l'ère informatique. Nous obtenons :

11111111 10110110 01100110 11111001 00000000 11111111 00000000 10000000.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
0	1	1	0	0	0	0	1	0	1	1	1	0	1	0	0

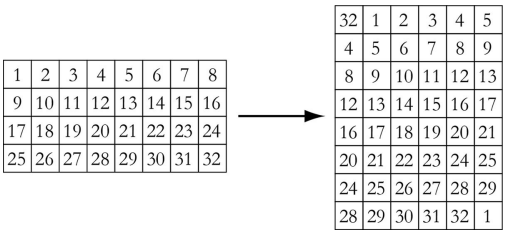
1	1	1	1	1	1	1	1	1	0	1	1	0	1	1	0
17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
0	1	1	1	0	1	0	0	0	1	1	0	0	0	0	1
0	1	1	0	0	1	1	0	1	1	1	1	1	0	0	1
33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
0	1	1	1	0	0	0	1	0	1	1	1	0	1	0	1
0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64
0	1	1	0	0	1	0	1	0	1	1	1	0	0	1	1
0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0

Transformation d’un bloc par la permutation initiale.

Le bloc fait alors l’objet d’un traitement en 16 « rondes », faisant chacune intervenir la clef de 48 bits correspondante déterminée ci-dessus.

Description d’une ronde

Une ronde part donc d’un bloc de 64 bits. Les 32 premiers bits forment le bloc de gauche et les suivants, celui de droite. Le bloc de gauche, ici « 11111111 10110110 01100110 11111001 », interviendra à la fin de la ronde. Le bloc de droite, ici « 00000000 11111111 00000000 10000000 », est étendu à 48 bits afin de se combiner à la clef. L’extension se fait selon une procédure proche de la précédente.



1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

Extension du demi-bloc de droite en 48 bits.

De même que précédemment, un tableau permet d'effectuer cette extension à la main.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
0	0	0	0	0	0	0	0	0	0	0	1	0	1	1	1
17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0
1	1	1	1	1	1	1	0	1	0	0	0	0	0	0	0
33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0

Extension dans notre exemple.

Le bloc de 48 bits obtenu, ici « 000000 000001 011111 111110 100000 000001 010000 000000 », est ajouté à la clef, ici « 100110 110100 001011 101111 111111 000111 000001 110010 », bit à bit, comme dans la substitution de Vigenère. On obtient : « 100110 110101 010100 010001 011111 000110 010001 110010 ». On subdivise alors ce nouveau bloc en 8 mots de 6 bits. Chacun est transformé en un mot de 4 bits au moyen de la « boîte de substitution »

qui porte son numéro d'ordre (p. suivante) et selon la règle suivante.

Pour le premier « 100110 », on utilise la première boîte à la ligne 10 (premier et dernier bit de 100110), soit 2, et la colonne 0011 (bits médians de 100110), soit 3. On obtient 8, soit 1000. On fait de même pour les autres, ce qui donne : « 1000 0111 1100 0100 0110 1111 1110 0110 ».

S_1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

S_2	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
2	0	14	7	11	10	4	13	1	5	8	12	6	9	2	5	15
3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

S_3	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

S_4	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

Boîtes de substitution. Elles permettent de transformer un mot de 6 bits en un mot de 4. Soit, par exemple, 111001. Le premier et le dernier bit mis ensemble donnent 11, soit 3 en décimal, qui fournit la ligne à utiliser dans le tableau, les autres donnent 1100, soit 12 en décimal, ce qui fournit la colonne. Nous obtenons ici 14 dans la première boîte, soit 1110 en binaire, et 3 dans la huitième, soit 0011.

S_5	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

S_6	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
2	6	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

S_7	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
3	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

S_8	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

Nous obtenons huit mots de 4 bits, soit un mot de 32 bits en les mettant bout à bout, ici « 1000 0111 1100 0100 0110 1111 1110 0110 ». Ce mot subit alors une permutation :

1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32

→

16	7	20	21	29	12	28	17
1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9
19	13	30	6	22	11	4	25

Permutation d'un mot de 32 bits.

Cette permutation peut à nouveau être appliquée à l'aide d'un tableau.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	0	0	0	0	1	1	1	1	1	0	0	0	1	0	0
0	1	0	1	0	0	0	0	1	0	1	1	0	1	1	1

17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
0	1	1	0	1	1	1	1	1	1	1	0	0	1	1	0
0	1	1	1	0	1	0	1	1	0	1	1	1	0	0	1

Permutation du mot de 32 bits de notre exemple.

Pour finir la ronde, on additionne bit à bit la partie gauche du bloc de départ, ici « 11111111 10110110 01100110 11111001 », au mot de 32 bits sortant de cette dernière permutation, ici « 01010000 10110111 01110101 10111001 ». On obtient : « 10101111 00000001 00010011 01000000 ».

L'ensemble des rondes

On effectue ainsi 16 rondes, chacune impliquant une clef de 48 bits. On finit le chiffrement du bloc en effectuant la permutation inverse de la permutation initiale.

1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64

→

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

←

1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64

Permutation initiale et son inverse. Pour la calculer, on repère où se situe le bit 1 dans la permutation initiale (partie droite) et on note le numéro du bit dans la partie gauche. On trouve 40, que l'on note donc en premier, et ainsi de suite.

On obtient : « 11100110 00001000 01011100 01011110 01010001 11001011 00100111 00011001 ».

Faiblesse du DES

Comme nous venons de le voir, aucun mystère ne plane sur l'algorithme de chiffrement de DES, il est parfaitement connu. De ce point de vue, il répond strictement au critère de Kerckhoffs : sa sécurité ne dépend que de la clef de 56 bits qu'expéditeur et destinataire du message s'échangent. Une clef de 56 bits peut prendre 2^{56} valeurs distinctes. Malgré l'énormité du nombre, qui s'écrit 72 057 594 037 927 936 en décimal, on peut imaginer attaquer un message chiffré de façon frontale et essayer dessus toutes les clefs

possibles l'une après l'autre. On parle alors de recherche exhaustive ou d'attaque par force brute.

Bien entendu, l'examen doit pouvoir se faire automatiquement, ce qui dépend du type de contenu du message. S'il s'agit d'un texte français traduit en code ASCII sur 8 bits, l'indice de coïncidence et les calculs de fréquences permettent de reconnaître de façon automatique si la clef est la bonne. En moyenne, il faut donc 2^{55} essais pour décrypter le message, puisque la découverte de la clef peut se produire à tout moment entre le premier et le dernier essai (le numéro 2^{56}).

Ce nombre est colossal, mais, de nos jours, un simple ordinateur de bureau analyse plusieurs millions de clefs par seconde. Il ne pourra pas casser seul un message (il lui faudrait plusieurs centaines d'années pour cela), mais des milliers d'ordinateurs mis en réseau peuvent y parvenir en quelques semaines, voire quelques jours.

Cette possibilité a poussé certains services de renseignements comme la NSA ou, au contraire, des ONG concernées par les libertés comme EFF (Electronic Frontier Foundation) à fabriquer spécialement une machine uniquement pour montrer que l'algorithme DES n'offrait plus la sécurité requise. Par exemple, la machine Deep Crack de EFF, qui avait coûté moins de 200 000 euro à la fin des années 1990, pouvait décrypter un message en quatre jours. Pour cette raison, l'algorithme DES a été largement abandonné au début des années 2000. Il reste cependant utilisé pour certaines applications, comme le cryptage de chaînes de télévision, qui voient leur clef changée régulièrement.

En 1993, le cryptologue japonais Mitsuru Matsui, chercheur à Mitsubishi Electric, a trouvé une attaque théoriquement plus rapide que la méthode exhaustive pour casser DES, mais elle demande d'utiliser 2^{43} couples clair/chiffré avec la même clef, ce qui la rend quasiment impossible en pratique : qui enverrait autant de messages ?

La méthode de Matsui passe par la résolution d'équations linéaires vérifiées par la clef, c'est pourquoi elle s'inscrit dans la sous-discipline de la cryptologie nommée cryptanalyse linéaire.

Le triple DES et l'AES

Pour pallier cette faiblesse du DES, on a imaginé de le tripler (c'est-à-dire l'appliquer trois fois) en recourant à deux ou trois clefs DES, ce qui le met à l'abri des attaques exhaustives telle celle que nous venons de voir. Cependant, la lenteur de l'algorithme a fait qu'il a laissé la place à un nouvel algorithme : l'AES (*Advanced Encryption System*, ou « norme de chiffrement avancé » en français). Celui-ci opère sur des blocs de 128 bits avec une clef de 128 bits. Il est donc pour l'instant à l'abri d'une recherche exhaustive. Bien que fondé sur des principes similaires au code DES, il donne un algorithme plus rapide. Nous ne le développerons pas ici, mais ses détails figurent sur Internet. À moins de commettre une erreur lors du protocole, il peut être considéré comme sûr. Il existe énormément d'autres alternatives du même type (que DES et AES), parmi lesquelles l'algorithme IDEA. (*International Data Encryption Algorithm*) qui est devenu courant et sert de fondement à certains logiciels de messagerie chiffrée.

Nous voyons donc que, même s'ils sont impossibles à exécuter à la main, les chiffrements par blocs sont les héritiers des chiffrements historiques, ceux des deux guerres mondiales et même de la Renaissance. On parle aujourd'hui de chiffrements symétriques, par opposition aux chiffrements asymétriques inventés dans les années 1970, que nous étudions précisément au chapitre suivant.

13 La magie des chiffres asymétriques

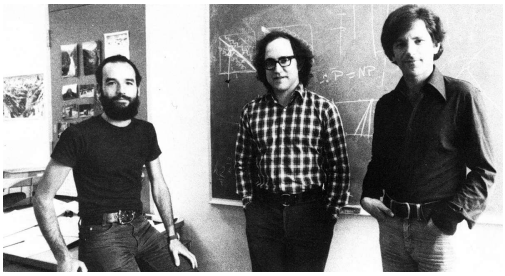
Dans tous les chiffres ou codes que nous avons rencontrés jusqu'à présent, savoir coder implique de savoir décoder : si on sait, par exemple, qu'un texte a été chiffré par un décalage de trois lettres, pour le déchiffrer, il suffit de décaler le message de trois lettres dans l'autre sens. Chiffrement et déchiffrement sont symétriques. C'est pourquoi ce type de chiffre est dit à clef symétrique, voire à clef secrète : la connaissance de cette clef suffit pour le déchiffrer. Il semble étrange qu'il puisse en être autrement. Pourtant, il existe des chiffres où savoir chiffrer n'implique pas que l'on sache déchiffrer. Ces chiffres sont dits à clefs asymétriques. Ils sont très utiles pour les échanges de clefs ou le négoce sur Internet.

Prenons l'usage des cartes bancaires. Quand vous payez avec votre carte, le terminal envoie les données (montant de la transaction, votre identité et celle du commerçant) de manière chiffrée au centre de traitement. Le chiffre mobilisé peut donc être connu de tous ceux qui sont capables d'analyser les algorithmes contenus dans le terminal. Vouloir les garder secrets serait vain. Si ces données suffisaient pour déchiffrer le message, il serait facile de connaître vos identifiants et de vous escroquer. Ce type de raisonnement a poussé des mathématiciens à élaborer des chiffres à clefs asymétriques : même en connaissant la clef

de chiffrement, l'escroc ne pourra pas décoder le message ! Magique, mais vrai.

L'art de divulguer un secret

Quand Ronald Rivest, Adi Shamir et Leonard Adleman découvrirent une méthode simple et astucieuse pour réaliser un tel cryptosystème asymétrique, ils voulurent éviter que leur découverte soit interdite de publication par le gouvernement américain. Aussi ne la publièrent-ils pas d'abord dans une revue de mathématiques, mais dans la rubrique de jeux mathématiques de *Scientific American*, tenue par Martin Gardner, qui était connue et lue internationalement aussi bien par les amateurs de jeux que par les spécialistes. C'était une manière fort habile de divulguer la « méthode RSA » (leurs initiales) rapidement au monde entier, tout en s'affranchissant de la censure officielle en matière de cryptographie. Les spécialistes du secret sont bien les meilleurs experts pour le contourner !



De gauche à droite : Adi Shamir, Ronald Rivest et Leonard Adleman, les inventeurs de l'algorithme de chiffrement RSA.

Dans leur article, les trois mathématiciens proposaient d'envoyer un rapport détaillé à tous ceux qui le demandaient. Quand la publication parut en août 1977, elle ne passa pas inaperçue. L'Agence de sécurité intérieure

américaine intervint pour que les chercheurs interrompent leur généreuse offre, mais elle fut incapable de fonder légalement sa demande.

Il était d'ailleurs trop tard : Rivest, Shamir et Adleman venaient de publier en février 1978 leur découverte dans un journal académique. Ne lâchant pas l'affaire, le gouvernement américain tenta d'interdire la divulgation des cinq lignes de programme permettant la mise en œuvre de l'algorithme sur ordinateur. De nombreux universitaires ripostèrent en incluant ces cinq lignes dans la signature de leurs courriels ou les firent imprimer sur un T-shirt ! Le gouvernement finit par renoncer, et Rivest, Shamir et Adleman purent déposer un brevet pour leur système en 1982.

Principes du système RSA

L'idée de départ des inventeurs repose sur une difficulté mathématique, celle de factoriser les nombres. La clef publique est essentiellement le produit de deux nombres premiers, tandis que la clef privée est constituée de ces deux nombres.

Les nombres premiers et les nombres premiers entre eux

Un nombre premier est un nombre non divisible, sauf par 1 et lui-même. Les autres nombres sont dits composés. Ainsi 2, 3, 5 et 7 sont premiers, 4, 6, 8 et 9 sont composés. Les nombres composés peuvent être factorisés en produits de nombres premiers, ainsi : $4 = 2 \times 2$, $6 = 2 \times 3$, $8 = 2 \times 2 \times 2$ et $9 = 3 \times 3$.
Deux nombres sont premiers entre eux s'ils n'ont aucun diviseur commun (sauf 1). Par exemple, 6 et 5 sont

premiers entre eux, mais 6 et 10 ne le sont pas (2 est un diviseur commun).

En théorie, la clef publique contient la clef privée, mais, en pratique, si les nombres sont suffisamment grands, personne n'est capable aujourd'hui de la trouver. Cela tient à la difficulté de la factorisation des nombres. Rien de plus simple que de trouver que 6 est égal à 2 fois 3. Il est déjà beaucoup plus difficile de remarquer que le nombre à 12 chiffres décimaux 221 091 801 607 se factorise en 470 201 fois 470 207… Personne n'est en fait capable d'effectuer cette factorisation à la main. Un ordinateur bien programmé est nécessaire pour réaliser l'opération. En revanche, il est plus facile de vérifier que ces deux derniers nombres sont premiers et que leur produit est bien 221 091 801 607. Avec un peu de courage, nous pouvons même le faire à la main.

Une carte bancaire. Les 16 chiffres choisis par le groupement interbancaire figurent sur la carte. Leur chiffrement avec la clef privée est contenu dans sa puce. Ces deux indications permettent de l'authentifier. Si la clef privée reste secrète, il est impossible de contrefaire une carte bancaire. Si elle est découverte, cela devient facile. La sécurité repose donc sur une question cryptographique.

En 1983, le groupement des cartes bancaires a adopté la cryptographie RSA avec une clef publique de 320 bits (21

35987 03592 09100 82395 02270 49996 28797 05109 53418 26417 40644 25241 65008 58395 77464 45088 40500 94308 65999 en décimal). Un nombre que personne à l'époque n'était capable de factoriser…

Lorsque vous faites une demande de carte, votre banque produit un certain nombre d'informations qu'elle fournit au groupement. À partir de celles-ci, ce dernier forme le numéro à 16 chiffres visible sur la carte. Il le chiffre ensuite à l'aide de sa clef privée pour former un numéro d'authentification. Ces données sont stockées dans la puce de la carte. Quand, plus tard, vous insérez votre carte dans le terminal bancaire d'un commerçant, le traitement commence par une phase d'authentification. Les deux numéros (celui de la puce et celui visible sur la carte) sont lus et le terminal contrôle, par le biais de la clef publique, qu'ils correspondent. Ce calcul prouve au terminal que votre carte est bien officielle et autorisée à effectuer des paiements.

L'affaire Humpich

S'interrogeant sur la fiabilité des cartes bancaires, un ingénieur français, Serge Humpich, est parvenu à comprendre les mécanismes d'authentification que nous venons de décrire. En 1997, il factorisa le nombre utilisé par le groupement. Il montra en effet que 21 35987 03592 09100 82395 02270 49996 28797 05109 53418 26417 40644 25241 65008 58395 77464 45088 40500 94308 65999 est le produit de 1113 95432 51488 27987 92549 01754 77024 84407 09228 44843 et de 1917 48170 25245 04439 37578 62682 30862 18069 69341 89293.

Rien de prodigieux dans cette factorisation : Humpich a simplement exploité un logiciel de calcul dit « formel » en vente libre. Il lui a alors été facile, à partir d'un numéro d'identifiant pris au hasard, de calculer le numéro

d'authentification correspondant. Il conçut alors de fausses cartes bleues qui étaient acceptées par les terminaux, même si elles n'étaient pas liées à un compte bancaire. Comme leur puce répondait « oui » à n'importe quel code PIN, ces cartes prirent le surnom de « yescards ».

Comme Étienne Bazeries l'avait fait au XIXe siècle en dévoilant à la hiérarchie militaire qu'il savait décrypter leurs messages, Serge Humpich contacta alors le groupement interbancaire pour négocier sa découverte d'une faille dans le protocole des cartes bancaires. De façon très logique, le groupement agit d'abord comme l'armée en lui demandant de prouver ses dires. Humpich acheta 10 carnets de tickets de métro auprès d'un distributeur de la RATP à l'aide de 10 numéros de cartes bancaires inexistantes. Le groupement feignit alors de vouloir négocier, mais mena parallèlement une enquête lui permettant de remonter jusqu'à l'auteur de ces pratiques « frauduleuses ». Il ordonna une perquisition du domicile de l'ingénieur. En représailles, Humpich diffusa sa découverte sur Internet en juin 1999. Il fut ensuite condamné à dix mois de prison avec sursis en février 2000.

Finalement, une institution réputée rigide comme l'armée de la fin du XIXe siècle – qui avait enrôlé Étienne Bazeries plutôt que de lui faire un procès – était infiniment plus intelligente que ce groupement des cartes bancaires… qui a provoqué la divulgation du code en ligne. Il faut d'ailleurs être bien naïf pour croire que la sécurité peut se gagner devant un tribunal. On ne prévient pas une invasion en disposant des sens interdits aux frontières, et mieux vaut étudier les armes de ses adversaires, ce que proposait Humpich.

Malgré tout, le groupement interbancaire comprit la leçon puisque, pour combler la faille découverte par Humpich, il a dorénavant recours à un nombre de 232 chiffres décimaux. Le voici : 15 50880 80278 37692 98423 92150 07513 07878 47102 02152 06711 10279 31119 90113 87539 45534 59999 75760 53046 71735 85609 15975 55389 79740

89381 73344 04367 47047 80986 39006 99066 79096 72893 30814 05044 93596 95145 08676 23994 24934 40750 58927 00157 39962 37452 93632 51827. Cela semble suffisant jusqu'à ce que l'on parvienne à factoriser ce nombre. Sachant que l'on sait aujourd'hui factoriser des nombres de 200 chiffres décimaux, le compte à rebours est lancé et il est peu probable cette fois qu'un autre ingénieur indépendant prévienne le groupement interbancaire avant que des « yescards » réapparaissent…

RSA dans le détail

Venons-en aux détails du chiffrement RSA. Même s'il implique des opérations impraticables à la main, ses principes restent accessibles à qui possède une bonne culture mathématique. Tout d'abord, la clef est composée du produit N de deux grands nombres premiers et d'un nombre A, qui n'est pas choisi au hasard (voir l'encadré ci-dessous). RSA permet de chiffrer les nombres de 0 à N – 1 en les élevant à la puissance A, dont on ne garde que le reste dans la division par N. Cela explique que le chiffrement RSA est gourmand en temps de calcul, puisqu'il équivaut à une exponentiation, tandis que les chiffrements symétriques ont valeur d'additions. On le réserve donc au transfert des clefs des chiffrements symétriques (destinés à assurer la véritable communication).

Détails du chiffrement RSA sur un exemple simplifié

La méthode RSA consiste à choisir deux nombres premiers, 5 et 11 par exemple. On considère alors le produit des deux nombres qui les précèdent, soit 40 ici (4 × 10), et on choisit un nombre premier avec 40,

comme 3. La clef publique est prête, il s'agit du couple (55, 3). Pour chiffrer 51 par exemple, on calcule 51^3 = 132 651 = 2 411 × 55 + 46, le résultat est 46.

Décryptement d'un chiffre RSA

Le déchiffrement du chiffre RSA exige de connaître les deux facteurs du nombre composé constituant la première partie de sa clef publique. Son décryptement sans connaître sa clef privée demande en principe de retrouver les deux facteurs, qui permettent d'obtenir un nombre B. Le déchiffrement se fait alors comme le chiffrement, mais en remplaçant l'exposant A par B (l'encadré *Déchiffrement de RSA* montre comment). Les principes fondant la méthode RSA remontent à Pierre de Fermat (1601-1665), célèbre pour avoir énoncé un théorème d'arithmétique qui ne fut démontré qu'à la fin du XX^{e} siècle, et à Leonhard Euler (1707-1783), sans doute le plus grand mathématicien du XVIII^{e} siècle. Ces calculs font partie de la théorie des nombres, longtemps considérée comme un pur jeu de l'esprit.

Ainsi, le grand mathématicien Godfrey Hardy (1877-1947) était très fier de travailler dans ce domaine, qu'il pensait dépourvu de la moindre application pratique. Étant antimilitariste, il ne voulait pas contribuer, même indirectement, à la guerre. En 1940, il écrivit dans *Apologie d'un mathématicien* : « Il est improbable que l'on trouve des applications à la théorie des nombres et à la relativité générale. » Cinq ans plus tard, les premières bombes atomiques, fruits de la théorie d'Albert Einstein, explosaient. Aujourd'hui, la théorie des nombres est au cœur des systèmes de cryptographie, qui sont considérés comme des armes. L'utilité ne se décrète pas, elle se découvre !

Le décryptement de RSA repose donc sur la factorisation en nombres premiers. La méthode historique pour factoriser un nombre est de le diviser par tous les nombres premiers entre 2 et sa racine carrée. Ainsi, pour factoriser les nombres jusqu'à 1 000 000, il suffit de connaître les 168 nombres premiers inférieurs à 1000. Les méthodes modernes, bien que beaucoup plus rapides, restent coûteuses en temps.

Déchiffrement de RSA

Reprenons l'exemple simplifié de l'encadré sur les détails du chiffrement RSA. Pour déchiffrer, nous avons besoin de la factorisation du nombre 55, qui est 5×11, et d'un nombre b tel que $3\,b - 1$ soit divisible par 40 (3 et 40 sont les deux nombres rencontrés précédemment). On montre en mathématiques qu'un tel nombre existe car 3 et 40 sont premiers entre eux. On trouve que 27 convient puisque $3 \times 27 - 1 = 80$.
Le déchiffrement consiste à reprendre les opérations de chiffrement en remplaçant 3 par 27. Cela s'explique mathématiquement à partir de la relation « $3 \times 27 - 1$ est divisible par 40 », mais nous n'entrerons pas dans ces détails. Par exemple, 46^{27} = 78426 25107 57613 41737 78889 26050 47155 76381 27616, dont le reste dans la division par 55 est bien 51.

L'idée d'inviolabilité que l'on prête à la méthode RSA vient donc de l'expérience, ce n'est ni un fait démontré ni même un fait démontrable. La découverte de nouvelles méthodes de factorisation pourrait d'ailleurs être tenue secrète, dans le but de décrypter les messages d'autrui. Pour l'instant, on sait factoriser des nombres d'environ 800 chiffres binaires.

Un RSA à 1 024 chiffres binaires est peut-être encore sûr, mais, pour les questions sensibles, il est préférable d'utiliser des nombres de 2 048 chiffres binaires.

Ce Qu'il Faut Décrypter

Le numéro de compte

La fameuse banque Bohlwinkel utilise pour ses cartes bancaires un système RSA, de clef publique 49 808 911 et 5 685 669. Quand un client paie avec sa carte, celle-ci envoie son numéro de compte en le chiffrant avec la clef ci-dessus. On découvre que le chiffre d'un client est 44 150 104.
Saurez-vous trouver son numéro de compte ?

L'ordinateur quantique

Décrypter RSA avec les moyens actuels est considéré comme hors de portée dès que la clef atteint les 2 048 bits. L'avènement d'un véritable ordinateur quantique puissant changerait la donne. Un certain algorithme fonctionnant sur un tel ordinateur, l'algorithme de Shor, permettrait de décrypter RSA pour des clefs bien plus grandes, car son temps d'exécution est polynomial et non exponentiel (vis-à-vis du nombre de chiffres), et donc plus rapide et moins sensible à la taille de la clef. Cependant, la mise au point d'un ordinateur quantique pose des problèmes théoriques (et pratiques) profonds, et il n'est pas certain qu'il voie le jour dans un avenir proche.

Les courbes elliptiques

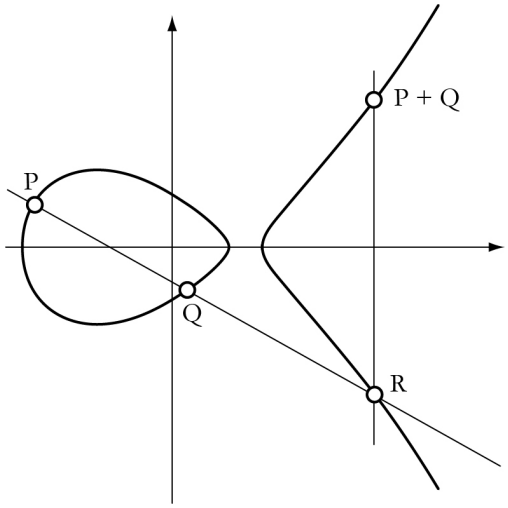
La recherche actuelle en cryptographie s'oriente vers des chiffrements du type RSA, mais plus subtils encore. Tous ces nouveaux chiffres s'appuient sur la théorie des groupes. Cette théorie a été introduite voilà deux siècles par Évariste Galois (déjà rencontré à propos de la machine Enigma), connu comme l'archétype du génie incompris de son vivant et pour être mort dans un duel stupide. Si les groupes ne lui servirent à rien en cette triste circonstance, ils sont devenus depuis les outils les plus utiles des mathématiques.

Les groupes les plus prometteurs en matière de cryptographie ont un fondement géométrique. Ils portent le nom de courbes elliptiques. Le rapport avec les ellipses, qui sont des cercles « aplatis » sur l'un de leurs diamètres, est indirect puisqu'il concerne le calcul de leurs longueurs. Nous n'insisterons pas davantage, ce point n'ayant aucun rapport avec la cryptographie.

Une courbe elliptique est une courbe dont l'équation est du type $y^2 = x^3 - 2x + 1$ complétée par un point, dit à l'infini, O. Sur une telle courbe, un procédé géométrique permet d'associer à deux points P et Q un autre que l'on note additivement P + Q. Cette « addition » possède certaines des propriétés de l'addition usuelle (voir l'encadré page précédente). Elle permet de définir la multiplication d'un point par un nombre positif : 2 P = P + P, 3 P = 2 P + P, etc. ou négatif : (–1) P = –P est le nombre tel que P – P = O, (–2) P = 2 (–P), etc. ainsi que la soustraction : P – Q = P + (–Q).

Une courbe elliptique

Le point « à l'infini » dans la direction de l'axe vertical est noté O. Si P et Q sont deux points de la courbe, on note PQ la droite les joignant. Cette définition admettant des cas particuliers, nous les traitons à part : PQ est la tangente en P si Q = P et la verticale passant par P si Q = O.



Si PQ n'est pas verticale, elle recoupe la courbe en un point R, on note P + Q le point où la verticale en R la recoupe. Si PQ est verticale, elle ne recoupe pas la courbe, on pose P + Q = O. De même, on pose : P + O = P.

L'addition définie ainsi est appelée une loi de groupe car elle vérifie les propriétés suivantes quels que soient les points P, Q et R de la courbe :

(P + Q) + R = P + (Q + R) (associativité)

P + O = P (O est un élément neutre)

Chaque point P admet un opposé P', c'est-à-dire tel que P + P' = O.

Dans ce cas, le groupe est dit commutatif car P + Q = Q + P.

Pour être utilisée en cryptographie, une courbe elliptique est limitée à un nombre fini de points, qu'on peut noter de 0 à N – 1. Ces points forment également un groupe, que l'on continue à appeler courbe elliptique. La détermination de ces points passe par des calculs algébriques, heureusement inutiles pour comprendre l'esprit de la méthode.

L'idée de départ est que le chiffrement consiste à transformer un point de la courbe. La clef secrète est constituée d'un point P de la courbe et d'un nombre entier, 3 par exemple. On calcule ensuite P' = 3 P. La clef publique est alors le couple de points (P, P'). Pour chiffrer un point M, le chiffreur choisit un entier, 23 par exemple, et transmet le couple (U, V) défini par : U = 23 P et V = M + 23 P'. La connaissance du premier nombre, ici 3, suffit pour retrouver M, car M = V – 3 U.

Pour retrouver le nombre choisi, 3 dans notre exemple, connaissant P et P', il suffit de savoir résoudre l'équation : P' = 3 P. L'utilisation du verbe « suffire » ne doit pas tromper. Cela ne signifie absolument pas que cela soit facile mais que, si vous savez le faire, vous savez décrypter. Le nombre 3 est alors appelé un logarithme discret, ce qui n'est guère intuitif si on adopte la notation additive ci-dessus. Avec une notation multiplicative de l'opération de groupe, cela devient plus habituel puisque l'équation s'écrit alors : $P' = P^3$. Dans l'ensemble des nombres usuels, 3 correspondrait au logarithme de base P de P', d'où le nom dans le cadre d'un groupe fini.

À l'heure actuelle, ce problème est considéré comme très difficile. On estime qu'une clef de 200 bits pour les courbes elliptiques est plus sûre qu'une clef de 1 024 bits pour la

méthode RSA. Comme les calculs sur les courbes elliptiques ne sont pas compliqués à réaliser, c'est un gros avantage pour les cartes à puce, des dispositifs qui disposent de peu de puissance et dont la taille de la clef influe beaucoup sur les performances.

La méthode a toutefois des inconvénients de deux ordres. D'une part, la théorie des fonctions elliptiques est complexe et relativement récente. Il n'est pas exclu que l'on puisse contourner le problème du logarithme discret. D'autre part, la technologie de cryptographie par courbe elliptique a fait l'objet du dépôt de nombreux brevets à travers le monde. De quoi rendre coûteuse son utilisation par les banques !

14 Comment sécuriser ses données informatiques

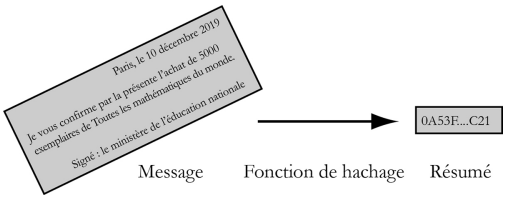
Chacun a rencontré ces pétitionnaires de rue qui font signer les passants sur des feuilles quasiment vierges. Et a été traversé du même doute : « D'accord pour signer, mais ma signature va vraiment servir la cause des réfugiés politiques du Burundi, vous êtes bien sûr ? » La question de la certification de documents a fait irruption dans le champ de la cryptographie quand, au mitan des années 2000, il est devenu possible de signer des publications électroniques, en particulier sa déclaration de revenus sur Internet. Déclarer ses impôts en ligne est pratique et rapide, mais a un inconvénient : tout devient immatériel. Dès lors, comment avoir confiance en un tel procédé ? Quelqu'un peut-il se faire passer pour vous ? Comment préserver le secret en se protégeant contre une fraude éventuelle ?

La signature électronique est la réponse à toutes ces questions. Le centre des impôts vous en accorde une quand vous vous connectez la première fois à son service. Pour l'obtenir, vous recevez d'abord un certificat électronique en échange de quelques renseignements, que vous êtes normalement seul à posséder. Certains figurent sur votre déclaration de revenus et d'autres sur votre dernier avis d'imposition. Vous devez également fournir une adresse mail valide. Vous obtenez alors une signature électronique qui garantit l'authenticité des documents transmis en ligne. Pour contrefaire cette signature, il faut posséder tous ces

éléments. C'est possible, mais difficile. Comment fonctionnent ces signatures et quelles sont leurs limites ?

Hacher pour sécuriser

Posons-nous d'abord une question simple : comment créer une signature électronique et à quoi correspond-elle ? L'idée est d'établir des résumés électroniques du document qui a été signé, afin plus tard de pouvoir vérifier que le fichier n'a pas été modifié. L'élément technique qu'on exploite est nommé une fonction de hachage. Il s'agit d'une application transformant une suite de bits en un résumé de longueur fixe, que certains nomment « haché » car la structure de ces fonctions fait effectivement penser à la technique de certains chefs pour découper les oignons !


Paris, le 10 décembre 2019
Je vous confirme par la présente l'achat de 5000 exemplaires de Toutes les mathématiques du monde.
Signé : le ministère de l'éducation nationale.
0A53F...C21
Message
Fonction de hachage
Résumé

Principe général d'une fonction de hachage : à partir d'un message (contrat ou autre), elle produit un résumé, en l'occurrence une suite de bits. Nous l'avons ici traduite en hexadécimal car c'est ainsi qu'elle apparaît normalement.

Ces fonctions doivent répondre à divers impératifs de sécurité. Tout d'abord, comme les résumés sont connus ou faciles à découvrir, ils ne doivent pas permettre de remonter aux originaux. Dans le cas contraire, cela pourrait entraîner des falsifications de signature. Cette propriété indispensable est appelée la résistance à la pré-image. Ce terme vient du langage mathématique associé aux fonctions. Le résumé est ici l'image du message par la fonction de hachage qui, lui,

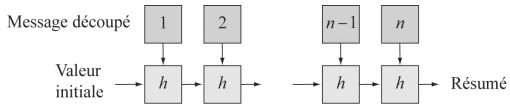
est la pré-image du résumé. Cette résistance ne suffit toutefois pas pour éviter la fabrication de faux.

Une bonne fonction de hachage doit également satisfaire la propriété qu'il est difficile de trouver un autre message ayant le même résumé (et ce, même si l'on connaît votre message). Si ce n'était pas le cas, alors n'importe qui pourrait fabriquer un faux contrat et prétendre que vous l'avez signé, puisqu'il a le même résumé. Cette résistance est nécessaire pour éviter la contrefaçon.

Enfin, une fonction de hachage doit assurer la résistance aux collisions. Dit autrement, il doit être difficile de trouver deux messages ayant le même résumé. Si ce n'est pas le cas, il est possible de vous faire signer un contrat et de prétendre que vous en avez signé un autre de même résumé. Remarquez que la résistance aux collisions implique le deuxième type de résistance (dit de résistance à la seconde pré-image).

De l'importance de la clef secrète

Ces principes étant posés, comment réaliser une fonction de hachage ? Comme souvent en informatique, l'idée est de la construire de façon progressive. Imaginons que nous disposions d'une fonction *h* fournissant un résumé sûr de 128 bits d'un message de 256 bits. Découpons alors le message donné M en blocs de 128 bits : M_1, M_2, etc. Combinons le message initial de 128 bits à M_1 pour obtenir, grâce à *h*, un résumé de 128 bits que nous combinons à M_2. Nous obtenons un nouveau résumé de 128 bits. Recommençons avec M_3. En continuant ainsi, nous obtenons un résumé final de 128 bits, c'est-à-dire une fonction de hachage H résumant tout message en 128 bits.



Construction de Merkle-Damgård. Le message est découpé en blocs de 128 bits, puis on résume successivement des chaînes de 256 bits en partant d'une chaîne arbitraire, appelée la valeur initiale. Bien entendu, le procédé est généralisable en remplaçant 128 par n'importe quel nombre.

Les mathématiciens Ralph Merkle et Ivan Damgård (le premier est américain et le second danois) ont montré que, si *h* est résistante aux collisions, alors H l'est aussi ! On peut obtenir une telle fonction de hachage au moyen d'un chiffrement par blocs comme AES, puisqu'il combine une clef secrète de 128 bits à un bloc de 128 bits pour obtenir un bloc de 128 bits. Il suffit d'introduire la clef secrète comme valeur initiale de l'itération. La fonction de hachage obtenue est aussi résistante que le chiffrement. L'ennui, c'est que l'AES ou les fonctions de chiffrement en général sont longues à calculer. C'est pourquoi on a introduit des fonctions de hachage plus rapides, telles MD5 (*Message Digest*) sur 128 bits ou SHA-1 (*Secure Hash Algorithm*) sur 160 bits, qui utilisent des chiffrements simplifiés.

Malheureusement, les clefs des chiffrements sont trop courtes, ce qui autorise une attaque exhaustive. Le nombre de cas à analyser pour MD5 est ainsi de 2^{16}, ce qui est beaucoup trop faible à l'heure actuelle. Pour SHA-1, il est de 2^{60}, ce qui peut être atteignable en mettant un très grand nombre d'ordinateurs en réseau. Même s'il est possible d'améliorer ces attaques, SHA-1 est encore relativement sûr.

Une autorité pour la certification

Les signatures électroniques permettent ainsi d'authentifier l'origine et le contenu des messages sur

Internet, d'en assurer l'intégrité. Les chiffrements à clefs asymétriques, comme RSA, fournissent une autre méthode pour atteindre cet objectif. Imaginons que vous soyez en relation habituelle avec un site marchand. Vous vous connectez : comment votre navigateur peut-il savoir qu'il n'a pas été piraté et que c'est bien au bon site qu'il s'adresse ?

Une réponse est dans l'échange de clefs. Le site marchand aura conservé votre clef publique. Votre navigateur lui envoie un message à chiffrer, puis vous déchiffrez le message renvoyé avec votre clef privée. Vous vérifiez ainsi que le site possède bien votre clef publique. Inversement, le site peut vérifier votre identité.

L'inconvénient est que cette méthode ne fonctionne que si vous êtes déjà client du site. Si ce n'est pas le cas, on fait intervenir une autorité de certification, la plus connue étant *Verisign*. Votre navigateur produit auprès d'elle différentes informations personnelles, ainsi que votre clef de chiffrement publique. L'autorité de certification émet alors un certificat regroupant ces informations, un numéro de série, une période de validité, ainsi qu'une signature numérique qu'elle aura créée à l'aide de sa propre clef privée. Lors d'une transaction avec vous, le site commercial reçoit ce certificat. Il prend connaissance de votre clef publique et peut vérifier la validité du certificat à l'aide de la clef publique de l'intermédiaire de sécurité. En faisant confiance à ce tiers, le site peut ensuite vous accorder sa confiance. Bien entendu, le procédé fonctionne dans l'autre sens. Ces différents protocoles sont les bases permettant les échanges d'informations sécurisées sur Internet (les sites dont l'adresse commence par « https »).

Comment sont stockés vos mots de passe

Lorsqu'on intervient sur un blog ou un forum, il est très souvent nécessaire de se connecter afin de s'identifier. Le login utilisé est fréquemment notre adresse mail, et chacun choisit un mot de passe, souvent le même, trop souvent… Or ces logins et mots de passe sont enregistrés dans une base de données et quiconque a accès à celle-ci connaît vos identifiants favoris, ce qui lui permet d'usurper votre identité ! Ce risque est valable que vous vous connectiez à un site de rencontre, un forum d'amoureux des plantes, le Pentagone ou à un autre site à accès réservé. Découvrez les identifiants de l'administrateur du site du Pentagone et vous pourrez en principe y semer la pagaille ! C'est ce que s'est amusé à faire le pirate informatique britannique Gary McKinnon. Entre 2001 et 2002, il est parvenu à effacer un bon millier de mots de passe des ordinateurs du gouvernement américain (Pentagone, US Navy, US Army, NASA, etc.) !

Pour éviter ces fuites, l'usage veut que les mots de passe soient stockés dans la base de données précisément sous la forme de leur empreinte hachée : ceux-ci n'apparaissent donc pas en clair. Pour vous identifier, vous devez produire votre mot de passe, dont la version hachée est calculée afin d'être comparée à celle stockée dans la base de données. À cause de la résistance à la pré-image, il est difficile à un usurpateur de produire un mot de passe définissant la même empreinte ! On peut faire de même avec RSA, comme nous l'avons déjà vu.

En pratique, ces remarques montrent que les sites vous renvoyant votre mot de passe si vous avez perdu vos identifiants ne sont pas sûrs, car ils ne devraient disposer que de leurs versions hachées. Il vaut mieux qu'ils vous envoient un mot de passe provisoire, à usage unique, en vous demandant de le changer.

Mais comment casser un mot de passe ? Une façon toute simple est d'essayer tous les mots de passe classiques. Il existe ainsi des dictionnaires de mots de passe usuels :

mots courants de la langue natale de l'utilisateur comme « maison » ou « objet », prénoms, suites de chiffres « logiques » comme 123456, mots spécialisés et rares du domaine de l'utilisateur comme « acatalectique », etc. Les hackers disposent ainsi d'un grand nombre de dictionnaires que l'on trouve sur Internet. Il est aussi possible d'obtenir de l'utilisateur ses mots de passe en l'espionnant : une fois installés sur son ordinateur, des logiciels malveillants enregistreront les touches frappées… et au passage les mots de passe.

Un « niveau de confidentialité correct » : PGP

Et les mails ? Comment rendre leur échange sûr ? À partir des différents algorithmes que nous avons examinés, l'américain Philip Zimmermann a conçu un système permettant d'assurer une confidentialité correcte aux échanges sur le Web. Correcte seulement, pas parfaite, et c'est pourquoi il a nommé son logiciel PGP (*pretty good privacy*, « niveau de confidentialité correct » en français). Lorsqu'on chiffre un texte avec PGP, les données sont d'abord compressées, ce qui réduit le temps de transmission, mais surtout prive la cryptanalyse de ses armes classiques, comme la méthode du mot probable.

PGP crée alors une clef secrète de chiffrement par blocs IDEA. de manière aléatoire, puis chiffre cette clef au moyen de la clef RSA publique du destinataire pour la lui transmettre. Celui-ci est donc le seul à en disposer. PGP assure ainsi le transfert de fichiers, la signature électronique, la vérification de l'intégrité et de l'authenticité des messages, et la gestion des clefs.

Le danger des objets connectés

Ce recours à un chiffrement par blocs du type AES, avec transfert de la clef au moyen d'un chiffrement RSA, est classique à l'heure actuelle. Le procédé est en principe sûr, mais n'est pas utilisable sur les petits objets connectés et en particulier ceux qu'on implante dans le corps humain, je pense aux *pacemakers* ou aux pompes à insuline. La chaleur due à l'application de RSA serait source d'inconfort ! Il en résulte que les petits objets connectés restent délicats à protéger.

Les objets connectés sont donc des cibles faciles pour les pirates, qui constituent en les connectant entre eux des réseaux de zombies, ou *botnets*. Un botnet est un réseau d'ordinateurs dont des pirates se sont rendus maîtres pour lancer des actions malveillantes, telles que l'envoi de *spams*, des opérations de *phishing*, des attaques en déni de service ou des recherches exhaustives de mots de passe…

Cela semble relever de la science-fiction (« Vous voulez dire que ma brosse à dents est capable de m'envoyer des spams ? Impossible ! »), mais une telle attaque s'est déjà produite ! Selon Proofpoint, une société californienne de sécurité, la première cyberattaque d'envergure de ce type (750 000 spams) a eu lieu fin 2013. Le nombre d'objets connectés devant passer les 20 milliards en 2020 selon toutes les prévisions, le marché est immense… pour les pirates.

Si les objets connectés deviennent des outils pour les pirates, les données qu'ils contiennent sont aussi susceptibles d'être attaquées, tout simplement volées, voire modifiées. Votre vie la plus intime peut ainsi être exposée, des appareils cruciaux pour votre santé menacés, etc. Le pilulier connecté pourrait ainsi, par exemple, envoyer de fausses indications à votre médecin, le tensiomètre de celui-ci mentir sur votre tonus artériel… et ne parlons pas des *pacemakers* ! L'imagination des pirates étant sans limite, ils trouveraient ainsi un moyen de rançonner les hôpitaux, les

médecins ou les malades en menaçant de détraquer des instruments médicaux.

Sans noircir le tableau à l'excès, puisque les objets connectés constituent aussi une forme de progrès, il est nécessaire de comprendre qu'ils incarnent un problème de sécurité important, trop peu pris en compte à l'heure actuelle. Tout récemment, un hôtel en Autriche a par exemple été rançonné après qu'un pirate eut pénétré son système informatique pour modifier les clefs électroniques, interdisant aux clients d'entrer dans leurs chambres…

Ce Qu'il Faut Décrypter

Les mots de passe bordures

Sur le site du ministère de la Défense de Bordurie, les mots de passe sont composés de quatre chiffres et stockés par leur cube.
Le mot de passe chiffré de Plekszy-Gladz est 71 215 348 625.
Saurez-vous trouver son mot de passe ?

Cryptomonnaies

Autrefois, les monnaies reposaient sur l'or, métal précieux qu'on trouvait dans des mines. Une pièce d'or avait une valeur universelle qui dépendait de son poids, si bien que toute augmentation de la masse monétaire correspondait au minage de l'or ! Ce temps est révolu et une monnaie, en vulgaire papier ou des minerais sans vraie valeur, dépend maintenant de la confiance accordée à la banque centrale qui l'a émise. Quant à l'augmentation de la masse monétaire, elle dépend de décisions politiques, normalement liées à l'économie du pays émetteur. Si la

confiance disparaît, la valeur faciale des billets peut s'évanouir, comme on l'a vu en Allemagne dans les années 1920 ou au Venezuela il y a peu, où l'on trouve des sacs à main faits de billets tressés tant leur valeur est dérisoire !

Alors que l'hyperinflation s'installe, un nouveau type de monnaie est apparu à la fin des années 2000 : le bitcoin, une « cryptomonnaie ». Il annonce un retour aux sources puisque la création de monnaie dépend de « minages ». Mais que mine-t-on dans les mines du bitcoin ? Sur quoi repose cette monnaie ? La réponse a de quoi surprendre : on mine… des calculs !

Cette affirmation mérite d'être commentée par un retour aux sources du bitcoin, ce qui oblige à parler des chaînes de blocs. Ces chaînes de blocs dépassent le cadre des cryptomonnaies, mais la première *blockchain* ayant été créée pour le bitcoin, le mieux est de partir de cet exemple afin d'être concret.

Du point de vue cryptographique, l'essentiel est la notion de fonction de hachage que nous venons de découvrir. Le premier bloc de la chaîne du bitcoin a été créé le 3 janvier 2009 par Satoshi Nakamoto, dont on ignore la réelle identité et même la nationalité. Ensuite, à intervalles réguliers, un nouveau bloc est créé, comportant le hachage du bloc précédent et les nouvelles transactions. C'est cette création que désigne le terme « minage » : elle correspond à un travail de décryptement, difficile à effectuer mais facile à vérifier. Elle est récompensée par l'attribution d'un certain nombre de nouveaux bitcoins, le tarif étant fixé à l'avance. Il est actuellement de 12,5 bitcoins et est divisé par deux tous les quatre ans environ. Il ne sera plus que de 6,25 bitcoins en 2020.

Ces blocs sont recopiés dans chacun des ordinateurs du réseau et leur validité est vérifiable par tous (en chiffrant et non en décryptant) : il suffit de contrôler les hachages de toute la chaîne. Ainsi, le livre de compte du bitcoin est validé par le calcul, sans qu'il n'y ait une autorité

quelconque pour cela. Non sans conséquences toutefois : les calculs de minage sont de plus en plus gourmands en électricité, si bien que les mineurs ont intérêt à s'installer dans des régions en surcapacité de production électrique.

Nous n'entrerons pas plus loin dans les détails du bitcoin et des autres cryptomonnaies, qui sont une sorte d'équivalent numérique de l'argent liquide et, à ce titre, sont présentes dans bon nombre d'affaires criminelles, en particulier celles liées à Internet. Les rançons demandées par les hackers doivent ainsi être payées en cryptomonnaies. Pour conclure, voyons ce que l'actuelle présidente de la Banque centrale européenne, Christine Lagarde, en disait en septembre 2017 :

> Les monnaies virtuelles […] produisent leur propre unité de compte et leur propre système de paiement, et ces systèmes permettent des transactions de pair à pair, sans chambre de compensation, sans banque centrale. À l'heure actuelle, les monnaies virtuelles comme Bitcoin ne représentent pas encore de menace pour l'ordre existant des monnaies fiduciaires et des banques centrales. Pourquoi ? Parce qu'elles sont trop volatiles, trop risquées, trop énergivores, parce que les technologies sous-jacentes ne sont pas suffisamment scalables [mal adaptées au changement d'échelle], que beaucoup d'entre elles sont trop opaques pour les régulateurs et que certaines ont été piratées. Mais beaucoup de ces défauts ne sont que des défis technologiques qui pourraient être surmontés avec le temps.

Le futur des chaînes de blocs

Le principe des chaînes de blocs est de se passer des intermédiaires centralisés et de permettre une interaction « pair à pair ». Pour en concevoir une, il faut imaginer un grand cahier que tout le monde peut lire librement et gratuitement, sur lequel tout le monde peut écrire mais où on ne peut rien effacer et qui est indestructible. Pour les cryptomonnaies, chaque page contient les transactions du jour.

Avec un peu d'imagination, il serait donc possible de remplacer par des chaînes de blocs toutes les centrales de

réservation hôtelière, de voitures avec chauffeur, de locations de vacances, etc. De même, elles pourraient servir à mettre en relation des producteurs locaux d'énergie (par énergie solaire) sans passer par un distributeur centralisant le tout. Dans certains pays sans cadastre, les chaînes de blocs garantiraient la propriété des terres et éviteraient les appropriations frauduleuses, puisque tout y serait noté de manière infalsifiable. Les chaînes de blocs sont capables d'assurer la propriété de tout ce qui est échangeable. De plus, elles sont très difficiles à falsifier, puisque les enchaînements sont facilement vérifiables. En fait, il faudrait pour cela que plus de la moitié des pairs passent un accord pour mentir. Ce risque semble suffisamment faible pour qu'on puisse prédire un avenir à ces outils…

Comment sécuriser un nuage

Cloud computing, stockage sur le *cloud*, jeu vidéo dématérialisé, calculs… : les « nuages » informatiques ont le vent en poupe. Leur intérêt ? Externaliser des ressources. Mais, si la sécurité des données échangées avec les serveurs ne pose pas de problèmes pour les photos du petit-neveu, ses recettes de cuisine ou une partie sur la dernière console de jeux, il en va autrement de celles des logiciels professionnels. Imaginez que vous écriviez votre prochain rapport sur un traitement de texte en ligne : comment être sûr qu'il ne sera pas lu en chemin par autrui ? Et *quid* d'une société d'ingénierie qui a externalisé sur des serveurs d'Amazon ou de Microsoft ses calculs de structure pour un nouvel avion ? Des regards indiscrets sont-ils susceptibles d'espionner son travail ?

C'est l'inconvénient actuel de l'informatique dans les nuages : elle souffre d'un manque de confidentialité. Or les mathématiciens y travaillent : voyons quelques pistes où la cryptographie est d'un grand secours.

Calculer sur une version chiffrée des données

Pour sécuriser l'informatique dans le nuage, il est important de pouvoir chiffrer les données envoyées. Comme on va utiliser des mathématiques, remarquons que chiffrer revient en somme à appliquer une fonction f transformant un nombre en un autre, soit : $x \rightarrow f(x)$, comme vous l'avez sans doute remarqué si vous avez une culture mathématique. Les calculs vont alors se faire sur $f(x)$ et non sur x, c'est-à-dire sur le chiffré et non sur le clair. Par exemple, s'il s'agit d'une addition, nous calculons : $f(x) + f(y)$. Quelle fonction de chiffrement f choisir pour obtenir $x + y$ quand nous déchiffrons $f(x) + f(y)$? La condition la plus simple est que f vérifie : $f(x) + f(y) = f(x + y)$ pour tout x et y, c'est-à-dire que f soit un « homomorphisme additif » (c'est le terme mathématique consacré).

Le déchiffrement sera encore possible si : $f(x) + f(y) = f(x * y)$ où * est une autre loi, par exemple une multiplication. Nous parlerons encore d'homomorphisme additif dans ce cas. Un système de vote électronique est typiquement à même d'exploiter un tel chiffrement. Chaque vote est chiffré. Le déchiffrement de la somme des chiffrés fournit le résultat, sans que l'on déchiffre pour autant chaque vote. Pour le formuler autrement : vous pouvez connaître le résultat sans savoir comment chacun a voté.

De manière plus subtile, on peut également imaginer consulter une base de données dans le nuage (c'est-à-dire à distance, via Internet) sans révéler la requête faite. Soyons plus précis et supposons que nous disposions d'une base de quatre éléments M_1, M_2, M_3 et M_4 (pour fixer les idées, la méthode est la même pour 5, 10, 100, 1 000, etc.). Nous considérerons ces éléments comme des nombres entiers, puisque tout message est une suite de 0 et de 1. Aussi étrange que cela puisse paraître, la question est liée à un

calcul de polynômes. Plus précisément, soit le polynôme à quatre indéterminées :

$$P(X_1, X_2, X_3, X_4) = M_1.X_1 + M_2.X_2 + M_3.X_3 + M_4.X_4$$

Si nous voulons atteindre l'élément M_2, il suffit d'évaluer ce polynôme pour $X_2 = 1$ et les autres X nuls car il donne M_2. Supposons que nous disposions d'un chiffrement homomorphe pour l'addition *f*. On en déduit :

$$P[\, f(X_1), f(X_2), f(X_3), f(X_4)\,] = f[\, P(X_1, X_2, X_3, X_4)\,].$$

Il s'agit donc d'évaluer le polynôme P pour $f(X_1)$, $f(X_2)$, $f(X_3)$, $f(X_4)$. En déchiffrant le résultat, on obtient P (X_1, X_2, X_3, X_4), c'est-à-dire M_2.

Bien entendu, cette méthode est difficilement applicable telle quelle si la base de données est significative, car les calculs deviennent gigantesques… mais l'idée est améliorable. De façon générale, la méthode permet d'évaluer tout polynôme de plusieurs variables et donc d'effectuer discrètement bien des requêtes possibles auprès d'un serveur.

De même, admettons que nous voulions faire effectuer le calcul : $x\ y + z$ dans le nuage (c'est-à-dire à distance, via Internet) sans révéler les valeurs de ces trois variables. Si nous disposons d'une méthode de chiffrement *f* homomorphe pour les deux lois, nous envoyons $f(x)$, $f(y)$ et $f(z)$ dans le nuage via le réseau. Le calcul : $t = f(x)\ f(y) + f(z)$ est effectué dans le nuage et la valeur de *t* est renvoyée. Cette valeur est déchiffrée, c'est-à-dire que l'on trouve *u* tel que : $t = f(u)$. Comme $f(u) = f(x)\ f(y) + f(z)$, l'homomorphie de *f* implique que : $u = x\ y + z$.

Nous voyons donc l'intérêt des chiffrements homomorphes : ils évitent de déchiffrer les données dans le cloud pour les manipuler. Grâce à cette astuce, on effectue les calculs sur les chiffrés et on ne déchiffre le résultat qu'une fois sorti du cloud. La confidentialité des données est

ainsi préservée, comme nous l'avons vu dans le cas du vote électronique.

Pistes de recherche

La recherche actuelle est active dans le domaine des chiffrements homomorphes, comme le montrent ces quelques exemples. Rappelons d'abord que le chiffrement RSA est homomorphe, mais seulement pour la multiplication, puisqu'il consiste à élever à une puissance. En s'inspirant de l'idée qui sous-tend ce chiffrement, Pascal Paillier a inventé, en 1999, un chiffrement homomorphe pour l'addition. À partir de deux chiffrés, il est donc possible de reconstituer le chiffré d'une somme.

L'existence d'un chiffrement doublement homomorphe sûr a été conjecturée dès 1978 par Rivest, Adleman et Dertouzos. Un cap théorique a été franchi en 2009 quand Craig Gentry, doctorant à l'université Stanford, a inventé le premier chiffrement doublement homomorphe et sûr. Malheureusement, l'avancée n'est que théorique, car la clef de son chiffre est très longue : plus de deux gigabits de données. Une taille qui rend ce chiffre impraticable ! La science a donc encore bien des progrès à effectuer pour que l'on puisse utiliser le *cloud computing* en confiance.

Conclusion

Nous voilà parvenus à la fin de ce long parcours à travers les codes secrets. Un point commun se dégage : chacun est constitué d'un algorithme de chiffrement et d'une clef. En cas d'utilisation intense, durant une guerre ou, de nos jours, dans le commerce sur Internet, il paraît proprement illusoire de vouloir conserver l'algorithme secret. Non : la partie secrète, c'est la clef.

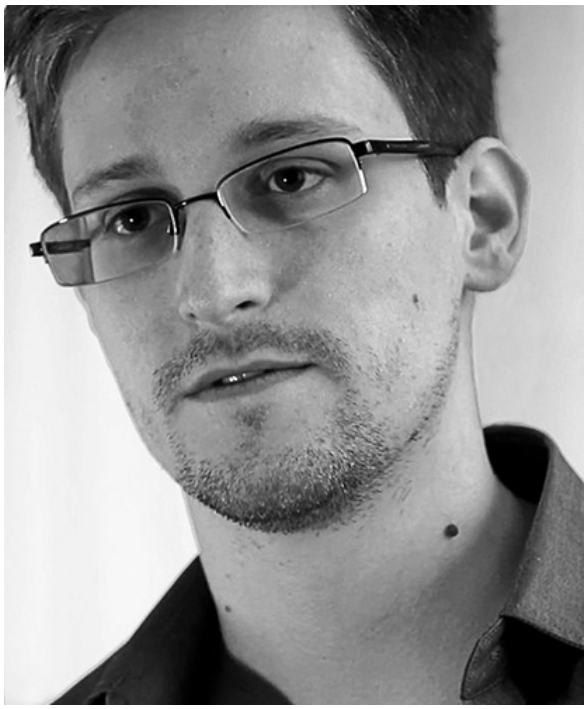
Son absence donne des chiffres très faibles dès lors que leur usage est étendu. De nos jours, on privilégie la clef aléatoire, afin qu'elle soit difficile à trouver et que la seule voie praticable pour décrypter soit sa recherche exhaustive. La force du chiffre tient donc à la taille de la clef (exprimée en nombre de bits, de nos jours), mais aussi à sa nature aléatoire. À l'époque classique, on recourait plutôt à des clefs faciles à retenir de tête, afin qu'elles ne puissent être lues par ailleurs par l'adversaire. C'était en fait une faiblesse, comme nous l'avons souligné, même si elle était compensée par les faibles moyens de calcul de l'époque.

Cela posé, nous avons montré que les chiffres sont de deux types, selon qu'il est effectivement possible de déduire l'algorithme de déchiffrement de celui de chiffrement, ou non. Dans le premier cas, c'est le fameux chiffre symétrique (car chiffrement et déchiffrement sont alors deux opérations symétriques) et, dans le second, le chiffre asymétrique. La différence tient ainsi à une difficulté calculatoire, qui dépend du matériel disponible et donc de l'époque. L'avènement de nouveaux moyens de calculs,

comme un ordinateur quantique puissant par exemple, pourrait bien changer la donne.

S'agissant des chiffres symétriques, deux techniques se distinguent : les substitutions alphabétiques et les transpositions. Le mariage des deux a donné lieu aux meilleures méthodes de la Première Guerre mondiale – je pense aux chiffres allemands de 1918 (ADFGX et ADFGVX), malgré tout cassés par Georges Painvin, le meilleur décrypteur de l'époque. De nos jours, ils ont donné lieu aux chiffres DES et AES, pour ne citer que les plus courants… et que vous utilisez sans le savoir quand vous naviguez sur Internet, pour votre déclaration d'impôts en ligne, par exemple.

En outre, les chiffres symétriques présentent un autre avantage au niveau calcul : ils s'exécutent dans un temps comparable à une addition (donc vite). C'est la grande différence pratique **[300]** avec les chiffres asymétriques connus, comme le RSA, qui s'exécutent dans le temps de calcul d'une exponentielle, donc lentement et avec un gros coût énergétique. De plus, les clefs des chiffres asymétriques sont plus lourdes que celles des chiffres symétriques pour une sécurité égale (pour être sûr, AES demande des clefs de 256 bits, contre 1 024 bits pour RSA). C'est pourquoi les chiffres asymétriques sont employés pour transmettre les clefs des chiffres symétriques, ainsi que pour des questions d'authentification. Si les clefs sont aléatoires et de taille suffisante, cette utilisation mixte donne des chiffres pratiquement indécryptables, même si le seul chiffre démontré théoriquement indécryptable (mais très lourd d'utilisation) est le masque jetable, exploité jadis par Che Guevara et le téléphone rouge.



En 2013, Edward Snowden a révélé la surveillance de masse assurée par la NSA.

L'idée que les chiffrements indécryptables que nous avons évoqués au long de cet ouvrage soient mis à la disposition de tous déplaît évidemment aux services de renseignements. Le gouvernement américain a, par exemple, exigé récemment d'Apple que la société révèle les clefs de chiffrements de ses téléphones aux enquêteurs du FBI. Une solution, pour satisfaire le désir de l'État de surveiller le crime organisé et les terroristes, serait de créer un tiers de confiance conservant les clefs de chacun et une législation prévoyant d'y faire appel dans le cadre de certaines enquêtes.

Selon le lanceur d'alerte Edward Snowden, la National Security Agency (NSA) américaine a préféré adopter une autre démarche et a demandé aux fournisseurs de logiciels américains de créer des portes dérobées, visant tout simplement à contourner leurs algorithmes de chiffrement. Mais cette exigence est problématique : elle ouvre une voie

d'accès pour pénétrer dans les citadelles numériques. La NSA a ainsi engendré une faiblesse dans tous les systèmes de chiffrements qu'elle contrôle : pourquoi les hackers se priveraient-ils de l'utiliser ?

La question est tout particulièrement préoccupante en matière commerciale. Les portes dérobées mises en place dans les algorithmes de chiffrements laissent en principe la NSA espionner le monde entier. Tant qu'il s'agit de la surveillance des trafics illégaux, l'objectif est noble, mais pourquoi l'agence américaine s'arrêterait-elle là si les renseignements glanés confèrent un avantage industriel ou commercial à une entreprise américaine, comme Boeing vis-à-vis d'Airbus par exemple ? Bien entendu, des entreprises de cette taille savent se protéger, *a priori*. Airbus sait très bien le faire, du moins ses cadres dirigeants l'affirment. En revanche, les sociétés de moindre envergure n'ont pas les moyens de s'offrir une sécurité informatique digne de ce nom. Quelles précautions peuvent-elles alors adopter ?

Pour éviter l'espionnage de la NSA ou d'autres agences, une précaution élémentaire est de s'assurer que les ordinateurs contenant des secrets industriels ou commerciaux ne soient pas reliés à Internet, ni raccordés à des ordinateurs eux-mêmes connectés au réseau. Les communications importantes doivent être chiffrées par un masque jetable de préférence, car c'est le seul chiffrement indécryptable, s'il est bien utilisé. Ces opérations de chiffrements doivent se faire sur cet ordinateur isolé d'Internet, sinon un cheval de Troie pourrait récolter la clef sur l'ordinateur. De même, à l'autre bout de la transmission, le déchiffrement doit s'effectuer sur un ordinateur isolé, seule riposte à l'espionnage organisé. Dans ce cadre, la transmission des clefs ne relève pas de la communication par Internet, mais par un échange physique. La faiblesse du procédé se situe ici.

Une autre idée est de se rendre invisible sur Internet pour conduire les négociations délicates où le secret est

nécessaire (de l'ampleur d'une fusion-acquisition de sociétés, par exemple). Il s'agit de devenir furtif et non plus de chiffrer ses données. Comment se dissimuler ? En utilisant des racines ouvertes dont les DNS (*Domain Name System*) ne figurent pas dans les serveurs de DNS usuels. Quelques sociétés commercialisent cette possibilité, dont Open-Root présidée par Louis Pouzin, l'un des pères d'Internet.

La guerre commerciale reste une guerre, et aujourd'hui, comme sur les champs de bataille de la Première Guerre mondiale, la victoire appartiendra à celui qui réussira à protéger ses secrets.

REMERCIEMENTS

Parvenu au terme de cet ouvrage sur les codes secrets, je voudrais avant tout remercier mes amis de l'Association des réservistes du chiffre et de la sécurité de l'information (ARCSI), dont bon nombre figurent comme auteurs dans la bibliographie. Je souhaiterais adresser une mention particulière à Daniel Tant, à qui j'ai emprunté quelques cartes chiffrées du début du XX^{e} siècle, à Jon D. Paul pour ses photographies de machines Enigma, entre autres, ainsi qu'à Jean-Louis Desvignes, le président de l'ARCSI, organisateur de passionnants colloques sur la cryptologie, qui m'ont inspiré. Je remercie également Éric Landgraf, qui m'a permis d'accéder facilement aux documents des Archives nationales ainsi qu'à celles de la ville de Strasbourg. Pour finir, je tiens à remercier ma fidèle relectrice, qui se reconnaîtra, et mon éditeur, Christian Counillon, qui m'a encouragé dans l'aventure qu'a été ce livre.

Ga rj ivhkjihj tiv vcawrkg h dtzj xqba vzz exlh qz ti npdwj ayuxc fz sswa

Pjwmi NIpsnek

CE QU'IL FAUT DÉCRYPTER : SOLUTIONS

Les phrases chiffrées de la préface

La première a été chiffrée par un simple décalage (E devient H, etc.) et la seconde en l'écrivant à l'envers. On obtient : « Cette première phrase est chiffrée par un simple décalage. »
« Cette seconde phrase peut être plus difficile à décrypter. »

Message dissimulé dans un livre

Le message est « évasion ce soir ». Chaque lettre du message a été marquée par un petit point plus clair.

Un message de César

Il suffit de décaler chaque lettre de trois positions dans l'ordre alphabétique inverse pour obtenir : « ATTAQUEZAQUATREHEURESPARLENORD »

Un message fleuri

En gardant les premières lettres des noms de fleurs, nous obtenons, en confondant « u » et « v » : « Ce soir, neuf heures ».

Une étrange prière

Le message caché est « sauve-toi ».

Message à Abélard

Abbé est le numéro 08 de la première page, notée 82 ici, lard est le numéro 14, sa page est noté 23, ce qui n'importe pas. Le dernier nombre apparaît donc à la page 82, c'est-à-dire la première, et 64 signifie « nous acceptons votre offre » d'où le sens du message : « Abélard, nous acceptons votre offre ».

Un chiffre pour Othon

Vu le destinataire du message, une hypothèse raisonnable est de supposer que son début signifie : « pour Othon Carsonfuhi », soit : pour : 405, ot : 125, on : 236, car : 052, son : 341, fu : 503, hi : 325
Reporté dans le message, cela donne :
Pour Ot on Car son fu hi Car ot son pour hi fu hi on
C'est-à-dire : « Pour Othon Carsonfuhi, carottes sont pourries, fuyons ».

Transmission de pensée

En utilisant le code proposé dans le texte, « Il fait beau mais froid » signifie 8, « Tu ne trouves pas », 2, « Oui », 0 et « Vous pensez pareil ? », 5. Le nombre transmis est donc 8205.

Message d'un cryptologue

Le calcul des fréquences ne donne rien de probant. En revanche, le seul mot présentant une lettre doublée est EJHH, qui

signifierait CHIFFRES. En reportant les équivalences ainsi trouvées, on obtient :

&**ESCHIFFRES** R**RS**D**SII**&**S** O&& %RHD**EI**S**EES**& R**SSRS**

Le chiffre s'écroule alors assez vite, & est L, est U, R est P et est A. On obtient rapidement :

Les chiffres par substitutions mono-alphabétiques ne sont pas sûrs.

Un message maçonnique

Le message signifie : « notre code est fragile ».

Un message pour vous

Pour l'analyse, le mieux est de substituer les symboles par des lettres :

AB CBDED BFBGAEAB HBIGJED IKLM CBGNBDDGB HB HBIBOEG LO PM HL HBAKHPQB

Le calcul des fréquences montre que B représente E, nous obtenons :

A**E** C**E**DED **E**F**E**GAEA**E** H**E**IGJED IKLM C**E**GN**E**DDG**E** H**E** H**E**I**E**OEG LO PM HL H**E**AKHPQ**E**

La suite « DDG » entre deux E ne peut donc être que « TTR », d'où :

A**E** C**ET**E**TE**F**ER**AEA**E** H**E**I**R**JE**T** IKLM C**ER**N**ETTRE** H**E** H**E**I**E**OE**R** LO PM HL H**E**AKHPQ**E**

Le mot « C**ER**N**ETTRE** » ne peut être que « PERMETTRE ». On en déduit que H est D E est I d'où :

A**EPETITE**F**ER**A**I**A**EDE**I**RJIT** IKLM **PERMETTREDEDE**I**E**O**IR** LO PM **D**L **DE**AK**D**PQ**E**

La suite est relativement simple, on obtient : « ce petit exercice devrait vous permettre de devenir un as du décodage ».

Les hommes dansants

Pour l'analyse, le mieux est de substituer les symboles par des lettres en rétablissant les espaces donnés par les drapeaux.

Cela donne :

> AB CDEB EBF GDHHBF EIJFIJKF BFK LICMAB I EBCGMLLNBN IOBC AI HBKGDEB EBF LNBPQBJCBF BK QJ RBQ E IFKQCB

La fréquence du B est égale à 18 sur 83, il représente donc le E. L'isolement du I et sa fréquence (8 sur 83) font qu'il représente A et de même E, D. En soulignant les lettres décryptées, nous obtenons :

> A**E** CD**DE** **DE**F GDHH**E**F **DA**JF**A**JKF **E**FK L**A**CMA**E** **A** **DE**CGMLLN**E**N **A**O**E**C A**A** H**E**KGD**DE** **DE**F LN**E**PQ**E**JC**E**F **E**K QJ R**E**Q **D** **A**FKQC**E**

La considération des mots de deux et trois lettres montre que A, F, K représentent L, S, T puis Q, J, U, N. Nous obtenons :

> **LE** CD**DE** **DES** GDHH**ES** **DANSANTS** **EST** L**A**CM**LE** **A** **DE**CGMLLN**E**N **A**O**E**C **LA** H**ET**GD**DE** **DES** LN**E**P**UEN**C**ES** **ET** **UN** R**EU** **D** **ASTU**C**E**

Il est alors facile de conclure. Nous obtenons : « Le code des hommes dansants est facile à déchiffrer avec la méthode des fréquences et un peu d'astuce ».

Tintinophilie

En gardant les deux premières lettres de chaque mot, on trouve : « déchiffrer est un travail laborieux ».

La langue de feu

Par rapport au javanais, « av » a été changé en « af », le message signifie « difficile de comprendre cette langue de feu ».

Le sianavaj

« Parler en sianavaj est délicat, le comprendre encore plus. »

Les chiffres d'Hervé et d'Hélène

Ce sont deux chiffres de César, l'un transforme R en V et l'autre L en N d'où l'échange :

> Hélène. Rendez-vous dimanche, onze heures. Bises. RV

D’accord. Bises. LN

Le chiffre de Cassis

Le chiffre de Cassis est un chiffre par décalage substituant 06 à K, et ainsi de suite dans l’ordre. Le tableau de chiffrement donne :

A	B	C	D	E	F	G	H	I	J	K	L	M
22	**23**	**24**	**25**	**00**	**01**	**02**	**03**	**04**	**05**	**06**	**07**	**08**
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
09	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**

Le message est donc : « rendez-vous à cinq heures au local ».

Un message pour le chevalier de Rohan

Les amis du chevalier de Rohan ne lui avaient pas simplifié le travail, car aucune lettre ne se détachait vraiment en termes de fréquence. Sur 30 lettres, L se trouve 5 fois, G et U 4 fois. Cependant, le découpage des mots milite pour le fait que G représente E, puisque le premier mot est MG, qui se trouve être LE. Le début du décryptement est donc :

LE DULHXCCL**E**U **E**HJ YXUJ L**L** CT UL**E**E ALJ

Le digramme L**L** est probablement IL et le trigramme **E**HJ, EST. On obtient :

LE DU**IS**XCC**IE**U **EST** YXU**TIL** CT U**IE**E A**IT**

La lettre doublée C est une consonne, ni S, ni T, ni L déjà pris. Il reste M et N. Nous essayons N et obtenons :

LE DU**IS**X**NNIE**U **EST** YXU**TILN**T U**IE**E A**IT**

Vu le contexte, le deuxième mot est PRISONNIER ce qui donne :

LEPRISONNIEREST Y**ORTILN**T **RIE**E A**IT**

On lit donc : « Le prisonnier est mort, il n'a rien dit. » Il est clair que le chevalier de Rohan n'avait rien d'un cryptologue émérite, ou alors le stress lui avait perdre toutes ses capacités !

Le message chiffré par l'Albatros

La table de déchiffrement est :

A	B	C	D	E	F	G	H	I	J	K	L	M
J	R	T	N	E	V	Q	M	P	W	Y	L	K

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
F	B	H	O	I	A	G	C	D	Y	S	U	Z

D'où le décryptement : « voici un chiffre très faible. »

Les correspondances du 20 février 1890

Le message d'indicatif C 21 est un message en style télégraphique surchiffré par un décalage de César d'amplitude 14. Le sens est : « Plus triste que jamais. Envie de me lever pour un long baiser. » Le style télégraphique initial donne une petite incertitude sur les termes exacts.
Le message d'indicatif LILI est chiffré comme vu dans le texte. Le sens est : « Aucune consolation, je ne veux rien que mon Lili ! Folie incurable ! Pense qu'à vous. »

L'épilogue des cartes à Léa

La carte décryptée dans le texte fournit la table de chiffrement utilisée. La voici :

1	2	3	4	5	6	7	8	9	10	11	12	13
	O	H	R	C		P	S	U	F		Q	L
14	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**	**26**
V	B		J	T	D	N	G	A	I	E	M	

Le 1er février : « Ma Léa adorée, je t'aime de toute mon âme et souffre loin de toi. Ta photographie est à la tête de mon lit. Mon premier regard le matin est pour toi, que je chéri tant. Adieu mon ange bien aimé. Un million de baisers ».
Le 9 février : « Mon amour, je suis aussi impatient de te revoir mais pourquoi t'ennuies tant ? Nous rattraperons le temps perdu quand je serais libre. Comment ce fait-il que je reçois tes cartes que le soir tandis que je les recevais le matin ? Un bon baiser ».
Le 18 février : « Ma chère Léa, je suis très peiné en lisant ta carte. Je ne pensais pas avoir mérité les reproches que tu m'adresses si je ne t'ai pas si bien embrassé à Vertus c'est que nous n'avons pas été seuls si longtemps ce n'est pas faute de t'avoir attendu dimanche voilà la récompense adieu ».

Un message littéraire

Le message a été chiffré par une substitution mono-alphabétique. La méthode des fréquences des lettres puis des digrammes contenant W (représentant E ici), ainsi que la recherche du mot probable « burlesque », plus un jeu de devinettes donne : « la confusion règne entre burlesque et grotesque. » Pourtant, il y a différence. Le burlesque appartient à l'histoire littéraire et constitue un genre que l'on peut cerner. Le grotesque n'est pas un genre. Il caractérise plutôt un type de personnages de roman.

Un message de Paris à Strasbourg

En utilisant le tableau de correspondances du texte et en regroupant les lettres par deux, on obtient pour la partie chiffrée : « Méfiez-vous de Lagarde ».

Un message philosophique

Le message a été chiffré par un carré de Polybe. La méthode des fréquences des lettres puis des digrammes contenant 14 (représentant E ici), ainsi que la recherche du mot probable « imbécile », plus un jeu de devinettes donne : « c'est parce que la vitesse de la lumière est supérieure à la vitesse du son que tant de gens paraissent brillants avant d'avoir l'air d'imbéciles. »

Le message d'Henri à Claire

En admettant que le début du message signifie « chère Claire » et la fin « Henri », nous obtenons les correspondances :

c	h	e	r	e	c	l	a	i	r	e	h	e	n	r	i
d	i		s	f	d	m		j	s		i		o	s	j
		2					**1**			**2**		**2**			

ce qui donne un chiffre semblant homophonique :

a	c	e	h	i	l	n	r
	d	f, 2	i	j	m	o	s
1							

La plupart des lettres sont décalées d'une seule lettre, une alternative de chiffrement semble réservée aux voyelles qui

peuvent être chiffrées par leur numéro d'ordre. On en déduit facilement le message : « Chère Claire, rendez-vous ce soir à l'heure habituelle place de la Bastille. Henri ».

L'entarteur masqué

Le message a été codé par une substitution mono-alphabétique homophonique. Avec l'hypothèse de l'énoncé, un certain nombre de lettres s'identifient et on obtient :

MOI L ENTARTEUR MASQUE Γ **AIME RI**E**I**W**ULISER LES** V**RETENTIEU**Y **QUI NOUS** S**OU**9**ERNENT OU SE** R**ONT A**VV**ELER** V**I**V**OLES LES** V**I**V**OLES** W **EST** E**U** V**I**V**EAU** 9**I**9**E LES TARTES**

Il suffit de jouer un peu aux devinettes pour obtenir : « Moi, l'entarteur masqué, j'aime ridiculiser les prétentieux qui nous gouvernent ou se font appeler pipoles. Les pipoles, c'est du pipeau. Vive les tartes ! »

Un chiffré Playfair connu

Le premier message chiffré donne les correspondances :

NU	IT	CA	LM	ES	UR	LE
FP	DS	NL	ER	TM	PM	ET
FR	ON	TE	ST	DE	NA	NC
CU	AF	OT	IS	KT	HP	CB
YG	EN	ER	AL	SA	NC	HE
VJ	AB	LM	LE	PT	CB	KA

Cela permet de reconstituer le carré de chiffrement. On remarque d'abord les correspondances du type LE ET car elle implique que L, E et T sont alignés dans cet ordre. Comme AL LE et TE OT, OALET sont alignés dans cet ordre à une rotation près.

Avec ce type de raisonnement, on reconstitue progressivement le carré :

T	O	A	L	E
S	U	P	R	M
I	F	N	C	B
D	G	H	J	K
Q	V	X	Y	Z

LO	OL	VS	TL	QD	AX	OM	ML
AT	TA	QU	EA	DI	XH	EU	RE
PQ	UP	CR	LN	AO	LB	AB	OQ
SX	SU	RL	AC	OT	EC	EN	TV
FC	DO	FL	EA	BA	AJ	LP	JQ
IN	GT	CO	LO	NE	LH	AR	DY

Soit : « Attaque à dix heures sur la cote cent vingt. Colonel Hardy «
Remarque : le X entre les deux S vient du chiffrement du digramme SS qui doit être scindé en SX et XS.

Le message de Kennedy

> PT BOAT ONE OWE NINE LOST IN ACTION IN BLACKETT STRAIT TWO MILES SW MERESU COVE X CREW OF TWELVE X REQUEST ANY INFORMATION.

Un chiffre affine

Ces subtilités calculatoires recouvrent une simple substitution alphabétique, peu importe que la clef soit représentée par deux

nombres *a* et *b*. Un petit calcul de fréquences permet de reconnaître le E, chiffré en R.

MFXEF SO**R**UF DIM**R**H H**R**O**R**H LADUU E**R**HFU UDS**R**H **R**HKO**R** S**R**KE**R** BN**R**O**R** HLADU UE**R**HY FEHNI HKDKN KDVSL **R**P**R**HH FX**RR**H KOVSL UFLDM **R**FO**R**L EZYK**R** E

Le digramme le plus fréquent commençant par R dans le message est RH. Il est donc probable que H représente S (voir *Les digrammes disent tout* p. 117). On arrive au début de décryptement en grand caractère gras :

MFXEF SO**E**UF DIM**ES SE**O**ES** LADUU E**ES**FU UDS**ES SE**KO**E** S**E**KE**E** BN**E**O**E** **S**LADU UE**ES**Y FEHNI **S**KDKN KDVSL **E**P**ESS** FX**EES** KOVSL UFLDM **E**FO**E**L EZYK**E** E

La suite « P**ESS** FX**E** » fait penser au mot « message ». Le chiffre s'écroule alors progressivement, on obtient finalement : « La grande faiblesse des chiffres affines est de n'être que des chiffres par substitution. Ce message est donc facile à décrypter. »

Le message du commandant Pulier

Sous l'hypothèse qu'il s'agit d'une substitution alphabétique utilisant des nombres de deux chiffres, on obtient le découpage :

10 00 02 04 14 13 12 07 00 02 03 00 19 13 17 00 19 00 07 05 11 20 14 00 11 00
20 14 05 21 04 07 23 03 00 01 00 16 05 21 05 03 11 11 04 19 09 00 17 07 00 19
05 09 03 00 07 13 05 07 00 24 14 11 04 07 09 07 00 09 00 13 00 07 00 19 09 07
00 09 00 01 05 03 19 05 06 03 19 05 11 00 05 03 19 13 03 20 14 00 11 00 12 07
00 01 03 00 07 16 05 21 05 03 11 11 04 19 09 00 24 25 05 13 13 00 14 07 13 09
00 11 03 17 19 00 20 14 04 03 20 14 00 11 00 09 00 21 05 24 25 00 01 00 19 21
20 14 03 00 21 05 03 21 05 13 12 04 21 04 07 19 04 19 00 13 04 03 21 12 05 13
09 00 01 05 09 03 02 03 13 03 04 19 10 00 11 05 03 24 00 12 00 19 09 05 19 21
06 05 03 21 07 00 11 00 02 00 07 12 05 07 01 00 13 21 07 04 14 12 00 13 10 00
02 04 14 13 12 07 03 00 09 00 09 04 19 19 00 07 09 00 13 04 07 09 07 00 13 12
04 14 07 11 00 07 00 01 12 11 05 24 00 01 00 19 21 09 00 24 00 09 00 21 05 24
25 00 01 00 19 21 05 06 03 19 20 14 00 24 00 11 14 03 20 14 00 10 15 05 03 01
03 13 01 00 07 00 19 21 07 00 01 00 19 05 07 09 13 00 07 00 19 09 05 13 05 02
04 19 00 04 14 03 11 07 00 24 00 02 07 05 09 00 01 04 03 09 00 19 04 14 02 00
05 14 08 04 07 09 07 00 13 21 04 14 07 00 21 07 00 01 12 11 05 24 00 09 14 12
14 03 13 05 06 03 19 05 11 00

Sur 400 groupes de deux chiffres :

00 **01** **02** **03** **04** **05** **06** **07** **08** **09**

79 **14** **08** **09** **22** **34** **04** **34** **01** **24**

10 **11** **12** **13** **14** **15** **16** **17** **18** **19**

04 **19** **12** **22** **21** **01** **02** **03** **00** **27**

20 **21** **22** **23** **24** **25**

08 **18** **00** **01** **10** **03**

00 représente le E

Les répétitions dans Spotorno (le o : o – o – – o) poussent à le chercher parmi les groupes de huit lettres sans 00. La lettre o est parmi les lettres fréquentes, mais pas les plus fréquentes. On cherche la répétition, on trouve 13 12 **04** 21 **04** 07 19 **04** ce qui donne des équivalences et le début de décryptement suivant, où les parties décryptées sont en caractères gras :

10 **E** 02 **O** 14 **SPRE** 02 03 **E NS** 17 **E NE R** 05 11 20 14 **E** 11 **E** 20 14 05 **TOR** 23 03 **E** 01 **E** 16 05 **T** 05 03 11 11 **ON** 09 **E** 17 **RE N** 05 09 03 **E RS** 05 **RE** 24 14 11 **OR** 09 **RE** 09 **E SE RE N** 09 **RE** 09 **E** 01 05 03 **N** 05 06 03 **N** 05 11 **E** 05 03 **NS** 03 20 14 **E** 11 **E PRE** 01 03 **E R** 16 05 **T** 05 03 11 11 **ON** 09 **E** 24 25 05 **SSE** 14 **RS** 09 **E** 11 03 17 **NE** 20 14 **O** 03 20 14 **E** 11 **E** 09 **E T** 05 24 25 **E** 01 **E NT** 20 14 03 **E T** 05 03 **T** 05 **SPOTORNONE SO** 03 **TP** 05 **S** 09 **E** 01 05 09 03 02 03 **S** 03 **ON** 10 **E** 11 05 03 24 **E PE N** 09 05 **NT** 06 05 03 **TRE** 11 **E** 02 **E RP** 05 R 01 **E STRO** 14 **PE S** 10 **E** 02 **O** 14 **SPR** 03 **E** 09 **E** 09 **ONNE R** 09 **E SOR** 09 **RE SPO** 14 **R** 11 **E RE** 01 **P** 11 05 24 **E** 01 **E NT** 09 **E** 24 **E** 09 **E T** 05 24 25 **E** 01 **E NT** 05 06 03 **N** 20 14 **E** 24 **E** 11 14 03 20 14 **E** 10 15 05 03 01 03 **S** 01 **E RE NTRE** 01 **E N** 05 **R** 09 **SE RE N** 09 05 **S** 05 02 **ONE O** 14 03 11 **RE** 24 **E** 02 **R** 05 09 **E** 01 **O** 03 09 **E NO** 14 02 **E** 05 14 08 **OR** 09 R **E STO** 14 **RE TRE** 01 **P** 11 05 24 **E** 09 14 **P** 14 03 **S** 05 06 03 **N** 05 11 **E**

Savone peut se trouver en **S** 05 02 **ONE** ce qui donne de nouvelles équivalences et :

10 **E VO** 14 **SPRE V** 03 **E NS** 17 **E NE RA** 11 20 14 **E** 11 **E** 20 14 **ATOR** 23 03 **E** 01 **E** 16 **ATA** 03 11 11 **ON** 09 **E** 17 **RE NA** 09 03 **E RSARE** 24 14 11 **OR** 09 **R E** 09 **E SE RE N** 09 **RE** 09 **E** 01 **A** 03 **NA** 06 03 **NA** 11 **E A** 03 **NS** 03 20 14 **E** 11 **E PRE** 01 03 **E R** 16 **ATA** 03 11 11 **ON** 09 **E** 24 25 **ASSE** 14 **RS** 09 **E** 11 03 17 **NE** 20 14 **O** 03 20 14 **E** 11 **E** 09 **E TA** 24 25 **E** 01 **E NT** 20 14 03 **E TA** 03 **TASPOTORNONE SO** 03 **TPAS** 09 **E** 01 **A** 09 03 **V** 03 **S** 03 **ON** 10 **E** 11 A 03 24 **E PE N** 09 **ANT** 06 **A** 03 **TRE** 11 **E VE RPA** R 01 **E STRO** 14 **PE S** 10 **E VO** 14 **SPR** 03 **E** 09 **E** 09 **ONNE R** 09 **E SOR** 09 **RE SPO** 14 **R** 11 **E RE** 01 **P** 11 **A** 24 **E** 01 **E NT** 09 **E** 24 **E** 09 **E TA** 24 25 **E** 01 **E NTA** 06 03 **N** 20 14 **E** 24 **E** 11 14 03 20 14 **E** 10 15 **A** 03 01 03 **S** 01 **E RE NTRE** 01 **E NAR** 09 **SE RE N** 09 **ASAVONE O** 14 03 11 **RE** 24 **E VRA** 09 **E** 01 **O** 03 09 **E NO** 14 **VE A** 14 08 **OR** 09 R **E STO** 14 **RE TRE** 01 **P** 11 **A** 24 **E** 09 14 **P** 14 03 **SA** 06 03 **NA** 11 **E**

Le début du texte pourrait être : « je vous préviens, général… », ce qui donne encore de nouvelles équivalences et on reconnaît des termes militaires comme bataillon, grenadiers, chasseurs de ligne, division et la ville de Finale. Voici finalement le texte clair retrouvé :

Je vous préviens, général, que le quatorzième bataillon de grenadiers a reçu l'ordre de se rendre demain à Finale, ainsi que le premier bataillon de chasseurs de ligne. Quoique le détachement qui était à Spotorno ne soit pas de ma division, je l'ai cependant fait relever par mes troupes. Je vous prie de donner des ordres pour le remplacement de ce détachement afin que celui que j'y ai mis me rentre. Ménard se rend à Savone où il recevra de moi de nouveaux ordres. Touret remplace Dupuis à Finale.

La scytale

La longueur du message est de 71 lettres qui, étant premier, n'est pas factorisable. Il est probable qu'il faille compter 72 lettres, ce qui fait 8 fois 9. En groupant le texte en mots de huit lettres, on obtient :

CAECINDR
EEAYRCEN
MTVTCELE
EEEAOHOU
SCCLNUNF
SRUEFIGR
AYNDETUV
GPEEREEL
ETSCETU

En le lisant en colonnes : « ce message a été crypté avec une scytale de circonférence huit et de longueur neuf. RVL ».

Le *rail fence*

On essaye deux lignes, ce qui donne un message incompréhensible. On passe alors à trois lignes, ce qui donne :

C S E E F P

E E S G A T C I F E A U

M A E H R R

N L C R I G

R I F N E U T O S I N S

A E S R L E

Autrement dit, en lisant en zigzag : « ce message a été chiffré par un rail fence sur trois lignes ».

La grille tournante

On remplit le carré, puis on lui applique la grille quatre fois en la faisant tourner. On obtient le message : « L'Allemagne va contourner la ligne Maginot ».

La grille tournante de côté huit

Il suffit de remplir un carré de côté huit avec le message et d'appliquer la grille de côté huit donnée dans le texte pour obtenir le décryptement : « Démarate prévient que les Perses vont attaquer la Grèce par les Thermopyles ».

Le message du centre de la Terre

On commence par regrouper les premières lettres : « .gninheLévreH.e » puis on continue avec les secondes : «

rretaledertnecu », les troisièmes : « aegayovelsnadem » et ainsi de suite : « mocérffihcegass », « emecretpyrcédài », « ssuérzevasuov,o » et « varB » ce qui donne :

gninheLévreH.e rretaledertnecu aegayovelsnadem mocérffihcegass emecretpyrcédài ssuérzevasuov,o varB

et en l'écrivant à l'envers, on obtient :

Bravo, vous avez réussi à décrypter ce message chiffré comme dans le voyage au centre de la terre. Hervé Lehning.

Un message en Übchi

La longueur du message est 49, celle de la clef, 7, nous divisons donc le message en groupes de 7 : « FDTONEF NXMIXSE RUORAED ELGEARN SATERUR TIERARE RHVOCIN » et nous les plaçons en colonnes dans l'ordre donné par la clef « LOYAUTE » :

L	O	Y	A	U	T	E
3	**4**	**7**	**1**	**6**	**5**	**2**
R	E	R	F	T	S	N
U	L	H	D	I	A	X
O	G	V	T	E	T	M
R	E	O	O	R	E	I
A	A	C	N	A	R	X
E	R	I	E	R	U	S
D	N	N	F	E	R	E

Nous écrivons alors ce tableau en lignes : « RERFTSN ULHDIAX OGVTETM REOOREI AACNARX ERIERUS DNNFERE » et reformons nos colonnes :

L	O	Y	A	U	T	E

3	**4**	**7**	**1**	**6**	**5**	**2**
O	R	D	R	E	A	U
G	E	N	E	R	A	L
V	O	N	R	I	C	H
T	O	F	F	E	N	D
E	R	E	T	R	A	I
T	E	R	S	U	R	A
M	I	E	N	S	X	X

Nous n'avons plus qu'à lire les lignes et éliminer les deux X finaux, qui sont manifestement des nulles, pour obtenir le message en clair : « ordre au général von Richtoffen de retraiter sur Amiens ».

Une prophétie dans *Moby Dick*

Il s'agit de l'annonce de l'assassinat d'Indira Gandhi… si on utilise les méthodes de Rips.

Un message en Trithème

Le message se décrypte en :
Le chiffre de Trithème est faible car il ne dépend pas d'une clef.

Un message en Bellaso

On reconstitue d'abord les cinq alphabets, ce qui donne :

RFTP	R	A	B	C	D	F	G	H	I	L
		T	E	M	N	O	P	Q	S	V	X

AGEQ	R	A	B	C	D	F	G	H	I	L	
		X	T	E	M	N	O	P	Q	S	V
BHMS	R	A	B	C	D	F	G	H	I	L	
		V	X	T	E	M	N	O	P	Q	S
CINV	R	A	B	C	D	F	G	H	I	L	
		S	V	X	T	E	M	N	O	P	Q
DLOX	R	A	B	C	D	F	G	H	I	L	
		Q	S	V	X	T	E	M	N	O	P

On applique ensuite le chiffrement avec la seconde clef :

Chiffré	QV	QFBHOIH	OA	TOGSHXNF	BIA	AG	DQSRBFHSQT
Clef	C	O	R	D	E	C	O
Clair	LA	REVNION	DE	DIMANCHE	EST	VN	TRAQVENARD

Le message est donc : « la réunion de dimanche est un traquenard ».

Un message sudiste

La clef étant « manchester bluff », le message est facile à déchiffrer. Voici :

> Gen'l Pemberton, You can expect no help from this side of the river. Let Gen'l Johnston know, if possible, when you can attack the same point on the enemy's line. Inform me also and I will endeavour to make a diversion. I have sent you some caps. I subjoin despatch from Gen Johnston.

Un message du Viêt Minh

Il s'agit d'un message chiffré en Vigenère avec la clef TINHA, d'où le décryptement :

> Acheminer munitions de cent cinq sur Dien Bien Phu Signé Giap

Un message en Vigenère

On considère le message obtenu en retenant chaque première lettre des groupes de cinq. La lettre majoritaire y est G, qui correspond donc à E : la première lettre de la clef est C. On recommence avec les secondes lettres et ainsi de suite. On trouve la clef : « Caire », le message décrypté est : « J'annonce à votre Majesté que depuis hier, les Russes sont tous soumis et que l'étau s'est refermé autour de la plus grande partie de l'armée russe : le XIII^{e}, le XV^{e} et le XVIII^{e} Corps d'armée sont détruits. Les pièces d'artillerie sont rassemblées dans les forêts. Le butin de guerre n'a pas encore été comptabilisé, mais il est extraordinairement important. Aux alentours, le I^{er} et le VI^{e} Corps ont également souffert terriblement. Ils se sont mis précipitamment en retraite vers Mlawa et Myszyniec ».
Il s'agit du message adressé par le général Hindenburg à Guillaume II après sa victoire à Tannenberg. Bien entendu, celui-ci n'était pas codé ainsi.

Le défi du neveu de Babbage

Le début du message « UVQV FFGEW » peut correspondre à « cher oncle ». Si on a affaire à un Vigenère, la clef est « SOMERSET ». Cette clef donne le message :

> CHER ONCLE
> RIEN N EST PLUS AISE A REALISER QUE CE QUE VOUS COMPRENEZ PARFAITEMENT. COMME VOUS SAVEZ COMMENT FAIRE, IL SERA AUSSI FACILE DE DECRYPTER CELA. BU NUCH AHCPO …

Il semble que le début du message ait été chiffré avec la clef « SOMERSET » et la fin avec une autre. La fin du message « PICCS » ressemble à la signature « Henry », ce qui correspond à la clef EPLUI. En fait, un essai infructueux montre que la clef supplémentaire est PLUIE et donne sur la seconde partie du message :

> EN MEME TEMPS CELA VOUS FERA UN PETIT PUZZLE POUR VOTRE CERVELLE.
> VOTRE NEVEU AFFECTUEUX.
>
> HENRY

Finalement, le message est :

Cher oncle,

Rien n'est plus aisé à réaliser que ce que vous comprenez parfaitement. Comme vous savez comment faire, il sera aussi facile de décrypter cela. En même temps, cela vous fera un petit puzzle pour votre cervelle.

Votre neveu affectueux.

Henry.

Un message en Beaufort

On observe de nombreuses répétitions : VDL à distance 45, MOJ à distance 9 et YJ à distance 21 (et d'autres). La clef semble pouvoir être de longueur 3. On découpe alors le message en trois mots, chacun pouvant avoir été chiffré par une substitution mono-alphabétique : « BILOY VRYOY KOYIY CYLMJ » : Lettre majoritaire Y (6 sur 20). Clef = Y + E = C
« WVHPW WWJJY HJNVJ PVYGJ » : Lettre majoritaire J (5 sur 20) suivi de W (4 sur 20). Clef = J + E = N. Avec W, clef A.
« RDIJP GFMYN MPNFP FDNRN » : Lettre majoritaire N (4 sur 20). Clef = N + E = R
La clef serait « CNR », ce qui donnerait un message déchiffré en : « brausorgo… » La clef n'est donc pas la bonne. La clef suivante serait « CAR », qui donne : « Beaufort. Jolie échelle. Mer forte. C'est force neuf. Mer calme. Force quatre. » Ce texte a un sens, donc nous avons trouvé la bonne clef.

Un autre message en Vigenère

La répétition de « EJ » permet de suspecter que la longueur de la clef est égale à 6. On procède alors comme dans le décryptement précédent. On trouve la clef « Arthur ». Le message décrypté est de Jules Verne (*La Jangada*) :

> Ces embarcations étaient des « ubas », sorte de pirogues faites d'un tronc creusé au feu et à la hache, pointues et légères de l'avant, lourdes et arrondies de l'arrière, pouvant porter de un à douze rameurs, et prendre jusqu'à trois ou quatre tonneaux de marchandises ; des « égariteas », grossièrement construites, largement façonnées, recouvertes en partie dans leur milieu d'un toit de feuillage, qui laisse libre en abord une coursive sur laquelle se placent les pagayeurs ; des « jangadas », sorte de radeaux informes, actionnés par une voile triangulaire et

supportant la cabane de paillis, qui sert de maison flottante à l'Indien et à sa famille.

Le message de Bazeries

Le triplet AWA se répète deux fois à une distance de 45 et le triplet UWT à une distance de 10, ce qui laisse penser que la clef est de longueur 5. Nous considérons alors les cinq groupes :

AKSMW WWWUA DJGKA KWJW
WQTWT QARIW BQKMN CTKT
AZNFQ CIGQA BFSZT ZGS
QKVKR MFVJJ FMUZZ GKJ
GGXHO PXJPG UWCEF UGU

La recherche de la lettre la plus fréquente dans chaque groupe ne suffit pas pour déterminer la clef, ce qui laisse penser que la lettre E est moins fréquente que la normale dans le clair. En revanche, la méthode de saint Urlo donne la clef « SIORC ». Cette clef fournit le clair :

IOMZE SILTE ALZEV UORTF ELCAM EIOVN ESUOV EJSEH CACSN IOMSE LTNOS RIRVU OCEDA SELIC IFFID SULPS ELSTE RCESS EL

En l'inversant, on obtient :

LE SSECR ETSLE SPLUS DIFFI CILES ADECO UVRIR SONTL ESMOI NSCAC HESJE VOUSE NVOIE MACLE FTROU VEZLA ETLIS EZMOI

Ce qui se décrypte en : « Les secrets les plus difficiles à découvrir sont les moins cachés. Je vous envoie ma clef. Trouvez-la et lisez-moi ».

Une recette périgourdine

La difficulté est de trouver la transposition. Nous faisons l'hypothèse qu'elle correspond à une écriture inversée, ce qui donne :

Y**FMQU** SHPJT WMJUZ EXSVX NSZHF BAYSG IPFRQ IW**FMQ U**ZQHJ OCEAS KHJIF GZWTP JFMWF GWYUS LILFW WXSTT JBLES HCRJV MYWSM TTBOI EZMHJ BMVAS HPJGI PJNXS NJZIE DTEHS HPJRI RXIVI YSZVN BMVFX WYYSH YSJMV WSLIH CORFQ TENGA IEAIV NBMVZ BMLJI ZIFIN VFWAV JHQVJ NTEQQ WSQZI MXGMD QSNSN SZIUC AIWOB IRDMV FHCVJ OUFNO VXJOD E**SHLI** QSNEN FMGZW ZIHIQ WJNTI KCQIU OZXWO VGMSA HJJQR LHAIH CVHJG XSZFK MSECE SHMKW OUQJG TENGA IERMY CXWYW GIYKF WMIOD E**SHL**I QSLIL IAXJF

Nous remarquons la répétition de FMQU à la distance 36 (notée en gras ci-dessus), celle de SHLI à la distance 100 (en gras ci-dessus) donc la longueur de la clef pourrait être un diviseur commun de 36 et de 100, c'est-à-dire un diviseur de 4. Si c'est le cas, les quatre textes suivants ont été chiffrés par un décalage de César :

YUJJX NFSFW UJAJZ JFULX JSJWT EJAJJ NEHJX YNFYS WHFNE NZJFF JJQQX QNUWR FJNJS QNZHJ KUWMJ LHJZS SWJNE CWKIS QLJ

où J est la lettre la plus fréquente. Elle représente donc le E, ce qui signifie que la première lettre de la clef est F.

FSTUS SBGRF ZOSIW FGSFS BHVSB ZBSGN JDSRI SBXSJ SCQGA BBIIW HNQZG SSCOD HOOOH SFWIN COOS JHCGF EHOGG RXGFO HSIF

où S est la lettre la plus fréquente. Elle représente donc le E, de sorte que la seconde lettre de la clef est O.

MHWZV ZAIQM QCKFT MWLWT LCMMO MMHIX ZTHIV ZMWHM LOTAI MMZAQ TWIMN ZABMC UVDLN MZQTQ ZVAQA VXKCM UTAMW IWDLL A

où M est la lettre la plus fréquente. Elle représente donc le E et la troisième lettre de la clef est I.

QPMEX HYPIQ HEHGP WYIWT ERYTI HVPPS IEPRI VVYYV IREIV VLIVV VESMD SIIIV VFXEI EGIWI IXGHR IHSME KQEIY YYMEI IX

où I est la lettre la plus fréquente. Elle représente donc le E, ce qui implique que la troisième lettre de la clef est E.
Ainsi, la clef est « FOIE », ce qui donne le message :

Trempez le foie gras entier dans un saladier rempli d'eau avec deux cuillères à soupe de gros sel pendant une heure. Épongez-le, dénervez-le, salez, poivrez. Placez-le dans une terrine. Rajoutez un verre de cognac. Laissez mariner une heure au frais, retirez l'alcool. Laissez le foie reposer à température ambiante avant de le faire cuire. Cuisez le foie par tranches de vingt secondes pour cinquante grammes. Laissez deux jours au froid avant de la déguster.

Un message en ABC

La longueur du message est 54, qui se décompose en 6 fois 9. On fait l'hypothèse que la clef est de longueur 6, ce qui fournit les six colonnes :

BEMVUREBF IKGEPBKVU RRRLCIMUR BELSOTENH BUJBFOBJF TCGTGWGJW

De trois en trois, la substitution est la même. Dans une même colonne aussi. Saint Urlo vient à notre secours. Dans la première

colonne d'origine, les lettres « ESAINTURLO » doivent représenter environ 80 % des lettres. Il s'agit des colonnes 3 et 4, qui correspondent donc au A et aux colonnes initiales 1 et 4. La même méthode convient pour B et C. Pour B, les lettres majoritaires sont « FTJOUVSMP », ce qui correspond aux colonnes 1 et 5, et aux colonnes 2 et 5. Pour C, il s'agit donc des colonnes 3 et 6. Nous obtenons ainsi les colonnes :

ADLUTQDAE GIECNZITS RRRLCIMUR BELSOTENH ATIAENAIE RAEREUEHU

Nous considérons la première ligne dans l'ordre 412536 :
« BAGARR ». On reconnaît le début de barrage. L'ordre est donc plus probablement 416532. En tableau :

B	A	R	R	A	G
E	D	A	R	T	I
L	L	E	R	I	E
S	U	R	L	A	C
O	T	E	C	E	N
T	Q	U	I	N	Z
E	D	E	M	A	I
N	A	H	U	I	T
H	E	U	R	E	S

Il ne reste plus qu'à lire le message : « Barrage d'artillerie sur la cote cent quinze demain à huit heures ».

Trois messages en ADFGVX

La longueur des messages est 66, soit 6 fois 11. Les messages 2 et 3 diffèrent en deux points distants de 33, multiple de la longueur des colonnes. Nous faisons l'hypothèse vraisemblable que cette longueur est 11 et donc que le nombre de colonnes est égal à 6. On découpe alors les messages en colonnes de 11. Les différences entre les messages 2 et 3 montrent que les colonnes 1 et 2 ont été placées en 3 et 6. Le message 1 est le

même que le message 2 avec une lettre en plus en tête. Cela permet de repérer la permutation faite, (1, 2) est devenu (3, 6), (5, 6) est devenu (1, 4) et donc (3, 4), (2, 5). Six permutations sont possibles. Nous pouvons les essayer toutes. Nous continuons ici avec celle qui a donné un résultat *a posteriori* 5, 4, 1, 6, 3, 2. En supprimant la permutation, les messages sont quasiment identiques avec la partie commune suivante :

FF DF GG DF AA DF DX GD DA DD DD DA GF AD AV GG DF AA AV GD DA AG DD DX DF AA XX FX AD DF GD

Nous lui appliquons la méthode du mot probable. Sous l'hypothèse que cette partie commence par « DIVISION ATTAQUE », nous obtenons à la suite : « V I S E N A ? T O I S ? ? U I N ». L'attaque doit donc viser Vis-en-Artois en juin. Il manque le jour, mais il est codé XX. Vu les clefs utilisées pour la substitution, il est probable qu'il ait gardé son sens de dernier chiffre, soit 9.

Un message d'Alberti

Pour décrypter, le plus simple est de fabriquer un cadran d'Alberti en photocopiant celui contenu dans ce livre en deux exemplaires. Il faut alors une paire de ciseaux pour découper les deux disques et une punaise ou une épingle pour faire pivoter le petit. Le message signifie : « Mon cadran est autoclave ».

Un message de Machiavel

On chiffre « DIVISER » avec chaque cylindre, on en déduit que le chiffrement de « DIVISER » en « TRUETFQ » n'est possible qu'avec l'ordre des cylindres suivant : 8/13/4/6, 8 ou 17/1, 2, 3, 15, 18 ou 20/1 ou 7/4 ou 6. Le cylindre 4 étant employé en troisième position, on en déduit que le dernier est 6. Finalement, on obtient 8/13/4/17/1, 2, 3, 15, 18 ou 20/4 ou 7/6. Cela permet de déchiffrer le message à partir de la position 21. On obtient « ERLA ?IS ». Nous faisons alors l'hypothèse que le ? représente D et que nous avons ici le début de « DISCORDE ». Le même

raisonnement que précédemment agrandit le lot des cylindres découverts. En reportant cela après le mot « DIVISER », nous pouvons continuer. Finalement, nous trouvons l'ordre des cylindres : 8, 13, 4, 17, 2, 1, 6, 10, 19, 3, 9, 15, 14, 5, 18, 11, 7, 12, 20, 16 et le sens du message « Diviser pour régner, semer la discorde, opposer ».

Un message de détresse

Pour décrypter ce message, il est nécessaire de disposer d'un ordinateur simulant une machine Enigma à trois rotors, ce que l'on peut trouver sur Internet. Pour les six dispositions des rotors, nous essayons chaque position, transformons le message, calculons son indice de coïncidence et gardons l'optimal. Nous trouvons que les rotors sont dans l'ordre III, I et II, et positionnés en C, W et B. Nous reprenons la méthode avec les connexions. Nous trouvons BN, CR, DQ, FW et KL. Le message est : « Première division. Nous tenons toujours mais subissons une attaque violente par une division de chars. Prière d'envoyer l'aviation. »

Un masque jetable qui porte bien son nom

Le mot probable « Du Haut Quartier Général » donne la suite de bits :

10001 00111 01010 10000 01101 00011 00001 11101 01111 01000 10000 01110
00111 10101 11000 01111 00101 11010 01101 00111 00101 11100 10010 00001
10011 11101 11011 10010 11000 01110 1100

Nous l'ajoutons au début du message chiffré afin d'en déduire le début de la clef :

10111 11001 00000 11010 00011 11110 11001 01010 11000 11111 10010 11001
00111 00101 10010 10101 10101 11110 10010 00111 11011 01100 11001 00101
10001 11011 10000 11011 01010 11001 0001

Le germe est une heure en seconde, donc un nombre compris entre 0 et 24 x 60 x 60, soit 86 400 c'est-à-dire 10101000110000000 en binaire. Nous avons donc 17 possibilités, entre 1, 10,…, 10111 11001 00000 11 en

conservant de 1 à 17 des premiers bits trouvés. En les essayant l'un après l'autre, on trouve qu'il faut en garder 16 ce qui donne le germe 48 705 soit 13 heures, 31 minutes et 45 secondes car le terme suivant est alors 339 699 032, soit 10100 00111 11101 10010 10101 1000. Le début de la clef est alors : 10111 11001 00000 11010 00011 11110 11001 01010 11000, ce qui correspond à ce que nous avons obtenu. En continuant, nous trouvons la clef complète :

10111 11001 00000 11010 00011 11110 11001 01010 11000 11111 10010 11001
00111 00101 10010 10101 10101 11110 10010 00111 11011 01100 11001 00101
10001 11011 10000 11011 01010 11001 00010 01010 11010 00110 10011 01011
11001 01011 01000 11101 10110 00111 11111 00111 10110 00110 11011 11101
01001 11110 11011 11111 10001 11001 01011 01110 10001 11001 10011 11101
01001 11010 01101 11011 10000 00000 10100 10100 00111 01111 00010 11001
10011 01011 00000 10000 10101 10011 01100 00101 11110 11001 01100 10110
01011 11111 11010 01100 11011 00011 00000 00001 10001 00101 01011 01101
01111 11100 00101 11001 01010 01010 10001 01101 11100

Le message en clair est donc :

10001 00111 01010 10000 01101 00011 00001 11101 01111 01000 10000 01110
00111 10101 11000 01111 00101 11010 01101 00111 00101 11100 10010 00001
10011 11101 11011 10010 11000 01110 11000 10000 01100 00111 10101 11110
00010 00001 10001 11101 11111 01101 11011 01110 00011 10111 01100 10011
00001 11011 10111 01001 11001 10100 00011 00100 11001 01010 00001 10010
01101 00111 10110 11010 01111 00111 10100 11101 11111 01110 11100 11010
00000 11101 00100 00011 01110 11011 11111 01001 11001 01100 10101 00000
11000 11110 11111 10010 01100 10101 00000 11001 01111 00111 11010 00100
00011 10000 11001 01111 00101 10001 10101 110

c'est-à-dire : « Du Haut Quartier Général aux commandants de divisions : notre code est percé ».

Le numéro de compte

Il s'agit de factoriser le nombre 49 808 911. Avec un logiciel adapté, on trouve 2819 multiplié par 17 669. De même, l'exposant à utiliser est 49 788 424 car son produit par 5 685 669 a pour reste 1 dans la division par 2818 fois 17 668. Le numéro de compte est 100 001.

Les mots de passe bordures

Il s’agit de la racine cubique de 71 215 348 625, soit 4145.

La phrase chiffrée des remerciements

La partie Pjwmi Nlpsnek est placée comme une signature. En supposant qu’elle signifie Hervé Lehning et qu’on est face à une substitution poly-alphabétique, la clef semble être « chiffre », ce qui donne la phrase :

> Et je dédicace cet ouvrage à vous tous qui avez lu ce livre jusqu’au bout. Hervé Lehning

GLOSSAIRE-INDEX

Les références en italiques concernent les paragraphes de l'ouvrage, les autres renvoient au glossaire.

ABC

Chiffre allemand de la Première Guerre mondiale, fondé sur un chiffre de Vigenère de clef « ABC » et une transposition de colonne.
Voir *Le chiffre ABC*, page 254, Vigenère, transposition.

ADFGX et ADFGVX

Chiffres allemands de la Première Guerre mondiale n'utilisant que ces lettres, car leurs codes Morse sont très éloignés.
Voir *Le chiffre ADFGX*, page 256, *L'ajout du V : le chiffre ADFGVX*, page 261.

AES

Advanced encryption standard. Algorithme de chiffrement moderne remplaçant le DES, aujourd'hui dépassé.

Voir *Le triple DES et l'AES*, page 354, DES

Al-Kindi

Al-Kindi est l'un des grands noms de la cryptographie. Il fut le premier à décrire la méthode des fréquences.
Voir fréquence.

Alberti

L'un des inventeurs des chiffrements poly-alphabétiques.
Voir cadran d'Alberti.

Aléatoire

Le mot latin *alea* signifie « jeu de dés ». En français, aléatoire signifie imprévisible, lié au hasard. Cette définition même montre qu'il n'est pas facile de fabriquer de l'aléatoire, ce qui est pourtant exigé par la méthode du masque jetable.
Voir masque jetable, pseudo-aléatoire.

Algorithme

Algorithme est la version mathématique, et rigoureuse, de recette. Comme en cuisine, un algorithme nécessite des ingrédients (en mathématiques, on dit des arguments) et une série d'opérations (en mathématiques, on dit des instructions élémentaires). Il a aussi un but : résoudre un problème donné. Par exemple, l'algorithme de l'addition fournit la somme de deux nombres à partir de ceux-ci, qui sont donc les arguments de l'algorithme.

Le mot algorithme vient du nom du savant arabe Al-Kwarizmi (780-850), qui fournissait ses méthodes sous forme algorithmique. Les méthodes de chiffrement correspondent toujours à des algorithmes précis.
Voir chiffrement.

Alphabet chiffré

Un alphabet chiffré réalise une correspondance entre l'alphabet usuel et des symboles destinés à les remplacer dans une substitution mono-alphabétique ou poly-alphabétiques.
Voir *Le message était de la poudre aux yeux*, page 18, *Un moyen mnémotechnique*, page 108, *Le premier chiffre à mot-clef,*page 202, *Blaise de Vigenère, un personnage multiple,* page 205.

Alphabet réversible

Alphabet chiffré tel que si Y chiffre X, X chiffre Y.
Voir *Un moyen mnémotechnique*, page 108, *Blaise de Vigenère, un personnage multiple,* page 205.

Analyse

Voir fréquence.

ASCII

American standard code for information interchange. Ce code traduit les caractères alphanumériques, c'est-à-dire alphabétiques ou numériques, en nombres entre 0 et 255.

Eux-mêmes sont écrits en binaire. À partir de ce code, tout texte devient une suite de 0 et de 1.
Voir *L'ère numérique et la cryptographie quantique*, page 329.

Asymétrique

Se dit d'un algorithme de chiffrement utilisant une clef publique pour chiffrer et une clef privée (différente) pour déchiffrer les messages.
Voir *La magie des chiffres asymétriques*, page 357, RSA.

Attaque

Toute tentative de casser un code. Une des formes d'attaques modernes est la recherche exhaustive de clefs ou de mots de passe. Elle consiste à essayer toutes les possibilités, éventuellement en les restreignant à un dictionnaire ou autre. Cette méthode est rendue possible par la puissance des ordinateurs et leur mise en réseaux.
Voir force brute.

Authentification

L'authentification consiste à s'assurer de l'identité de l'émetteur d'un message, mais aussi de l'intégrité du message reçu.
Voir *Principes du système RSA*, page 359.

Autoclave

Voir chiffre autoclave.

B-211

Machine à chiffrer électromécanique française de la Seconde Guerre mondiale, utilisée au niveau stratégique.
Voir *Les machines françaises*, page 321.

Babbage

Charles Babbage est un précurseur de l'informatique. Il s'est aussi intéressé à la cryptographie et a inventé la méthode connue sous le nom de Kasiski.
Voir Kasiski.

Bazeries

Étienne Bazeries est l'un des grands noms de la cryptographie. En particulier, il a décrypté le Grand Chiffre de Louis XIV.
Voir *L'arme de la guerre secrète*, page 13, *Le code Baravelli et l'affaire Dreyfus*, page 48, *Décrypter sans connaître le dictionnaire*, page 61, *Les correspondances personnelles du Figaro*, page 109, *Le mot probable de Bazeries*, page 238, *Le cylindre de Bazeries*, page 284.

Beaufort

Voir chiffre de Beaufort.

Bellaso

Voir chiffre de Bellaso.

Bigramme

Synonyme de digramme.
Voir digramme.

Bilitère

Voir chiffre bilitère.

Blockchain

Système utilisant la cryptographie pour authentifier des fichiers sans avoir recours à une quelconque autorité. Les blockchains ne se limitent pas aux cryptomonnaies comme le bitcoin.
Voir *Cryptomonnaies*, page 379.

Boîte à chiffrer d’Henri II

Bel objet de la renaissance probablement conçu pour effectuer un chiffrement poly-alphabétique.
Voir *Ma boîte à chiffrer d’Henri II*, page 278.

Boulanger

Voir chiffre de Boulanger.

Brute

Voir force brute.

C-36

Machine à chiffrer mécanique française de la Seconde Guerre mondiale, utilisée au niveau tactique.
Voir *La C-36*, page 324.

Cabinet noir

Service de renseignement des temps anciens chargé d'intercepter les lettres et de décrypter les lettres chiffrées.
Voir *Les cabinets noirs*, page 64.

Cadran d'Alberti

Cryptographe en forme de cadran contenant deux roues, permettant de réaliser des substitutions poly-alphabétiques.
Voir *Le cadran d'Alberti*, page 272.

Cadran de Wadsworth

Cryptographe en forme de cadran, permettant de réaliser des substitutions poly-alphabétiques dans lequel les roues ne sont pas divisées en le même nombre de symboles.
Voir *Les disques de Wadsworth,*page 275.

Camouflage

Technique consistant à cacher le sens des mots de façon convenue à l'avance, comme désigner le président de la République sous un nom anodin comme *tonton*. Cette technique ne trompe guère longtemps.

Voir *Les erreurs du Viêt Minh… et de leurs adversaires*, page 224.

Cardan

Voir grille de Cardan, chiffre autoclave.

Carré de Polybe

Carré 5 × 5 permettant de coder les lettres (sauf une) par des couples de chiffres.
Voir *Carré-ment bien*, page 122, *Cryptographie à l’« srevne » (à l’envers)*, page 250, *Le chiffre ADFGX*, page 256.

Casser

Casser un code signifie trouver sa clef ou, de façon plus générale, trouver un moyen d’accéder à ce qu’il protège sans y être autorisé.
Voir décrypter.

CD-57

Machine à chiffrer portative française de la guerre froide, utilisée au niveau tactique.

César

Chiffre correspondant à un simple décalage dans l’alphabet. Par exemple, un décalage de 3 consiste à remplacer A par D, B par E, etc.

Voir *Le César du meilleur chiffre*, page 28, chiffre, Rot13.

Chiffre

Ensemble de procédés (et de symboles) employés pour remplacer les lettres d'un message afin de le rendre incompréhensible… quand on ne connaît pas la manière de déchiffrer. On distingue généralement les chiffres par substitution et ceux par transposition.
Voir *Les chiffres par substitution*, page 103, *Les chiffres par transposition*, page 163, César, ABC, ADFGX, Übchi, Vigenère.

Chiffre autoclave

Chiffre pour lequel la clef est dans le message en clair.

Chiffre bilitère

Chiffre inventé par Francis Bacon, consistant à employer deux polices de caractères différentes, le message étant chiffré par ces différences de police et non par le texte écrit.
Voir *Le chiffre bilitère de Francis Bacon*, page 125.

Chiffre de Bazeries

Chiffre consistant en une substitution mono-alphabétique suivie d'une transposition.
Voir *Le chiffre de Bazeries*, page 253.

Chiffre de Beaufort

Chiffre poly-alphabétique utilisant une table de Vigenère, mais d'une autre manière.
Voir *Le chiffre de Beaufort*, page 210.

Chiffre de Bellaso

Chiffre poly-alphabétique inventé par Giovan Bellaso, premier à utiliser un mot comme clef.
Voir *Le premier chiffre à mot-clef*, page 202.

Chiffre de Boulanger

Chiffre mêlant substitution poly-alphabétique et transposition, utilisé par le général Boulanger.
Voir *La cryptographie à l'« srevne » (à l'envers)*, page 250.

Chiffre de la marine japonaise

L'un des chiffres de la marine japonaise pendant la guerre du Pacifique. Il consiste en un dictionnaire chiffré, surchiffré par une table de nombres aléatoires.
Voir *Le chiffre de la marine japonaise*, page 266.

Chiffre de Rozier

Une complication illusoire du chiffre de Vigenère.
Voir *Une complication illusoire : le chiffre de Rozier*, page 211.

Chiffre des émigrés

Chiffre homophonique utilisé par les émigrés en 1793.
Voir *Le chiffre des émigrés*, page 137.

Chiffre du livre

Utilisation d'un livre comme recueil de clefs.
Voir *Les espions allemands et le chiffre du livre*, page 223.

Chiffre zigzag

Chiffre par transposition consistant à écrire en zigzag.
Voir *Le chiffre* rail fence *ou zigzag*, page 166.

Chiffrement

Application d'un chiffre. Il s'agit d'un algorithme.
Voir algorithme.

Chiffrement homomorphe

Un chiffrement est homomorphe pour l'addition si la somme des chiffrés est le chiffré de la somme. De même, il est homomorphe pour la multiplication si le produit des chiffrés est le chiffré du produit. Il est doublement homomorphe s'il est homomorphe pour les deux opérations.
Voir *Calculer sur une version chiffrée des données*, page 383.

Chiffrer

Appliquer un chiffre.

Voir chiffrement, encodage.

Clef

Un algorithme de chiffrement nécessite habituellement une clef qui peut être un mot, une phrase, un nombre, etc.

Clef privée

Clef permettant le déchiffrement et donc restant secrète. Dans le cas d'un système symétrique, il s'agit de la seule clef. Dans le cas d'un système asymétrique, on la distingue de la clef publique permettant le chiffrement.
Voir *La magie des chiffres asymétriques*, page 357, clef publique.

Clef publique

Clef servant au chiffrement dans un système asymétrique, elle est accessible à tous ceux qui le veulent car elle ne permet pas le déchiffrement ; pour cela, il faut posséder la clef privée.
Voir *La magie des chiffres asymétriques*, page 357, clef privée.

Clef secrète

Clef dans un système symétrique ou clef privée d'un système asymétrique.
Voir *La magie des chiffres asymétriques*, page 357, clef privée.

Code

Système de symboles remplaçant des mots entiers. Les codes se distinguent donc *a priori* des chiffres mais, en pratique, les deux notions sont très proches et peuvent être confondues.
Voir *Chiffre ou code ?*, page 31, *La saga des dictionnaires chiffrés*, page 39.

Code pourpre

Code de la diplomatie japonaise pendant la guerre du pacifique.
Voir *Le code pourpre,* page 319.

Coïncidence

Voir indice de coïncidence.

Colossus

Premier ordinateur créé pour décrypter les messages de la machine de Lorenz.
Voir *La machine de Lorenz et Colossus*, page 318.

Confidentialité

Assurer la confidentialité de certaines informations, c’est s’assurer que seules les personnes autorisées y ont accès.
Voir *Comment sont stockés vos mots de passe*, page 376.

Connectés

Voir objets connectés.

Courbes elliptiques

Courbes permettant un chiffrement à clefs asymétriques.
Voir *Les courbes elliptiques*, page 366.

Cryptage

L’Académie française ne reconnaît pas ce mot et lui préfère chiffrement ou chiffrage. Cependant, il est d’usage, surtout dans le domaine de la télévision numérique, il n’existe donc aucune raison sérieuse de le bannir.

Cryptanalyse

Art d’analyser un message chiffré afin de le décrypter.
Voir décrypter.

Crypter

Version non académique du verbe chiffrer.
Voir cryptage.

Cryptogramme

Message chiffré ou codé.
Voir *Le mystère du scarabée d’or*, page 84.

Cryptographie

Étymologiquement, cryptographie vient d'« écriture cachée » (en grec). La cryptographie est donc destinée à cacher le sens des messages. Elle s'oppose à la stéganographie, qui s'efforce de cacher les messages eux-mêmes.
Voir *Vengeance de cœur*, page 21.

Cryptologie

Peut être pris comme synonyme de cryptographie, mais on scinde souvent la cryptologie en cryptographie et cryptanalyse.

Cryptosystème

Système de chiffrement complet incluant le transfert des clefs.

CX-52

Machine à chiffrer portative française de la guerre froide, utilisée au niveau tactique.

Cylindre

Machine à chiffrer manuelle.
Voir *Le cylindre de Jefferson*, page 283, *Le cylindre de Bazeries*, page 284, *La machine de Gripenstierna*, page 282.

Déchiffrement

Opération inverse du chiffrement quand on connaît la clef « légalement ». En ce sens, il s'oppose au décryptement où on découvre la clef par cryptanalyse.

Décryptage

Version non académique de décryptement.
Voir cryptage.

Décryptement

Action de décrypter.

Décrypter

Découvrir le sens caché d'un message sans en connaître la clef au préalable.

Delastelle

Le chiffre de Delastelle combine une substitution et une transposition.
Voir *La cryptographie à l'« srevne » (à l'envers)*, page 250.

DES

Data encryption standard. Algorithme de chiffrement des données moderne. Il est aujourd'hui dépassé et a été remplacé par AES
Voir *Le triple DES et l'AES*, page 354.

Dictionnaire

L’attaque de mots de passe par dictionnaire consiste à essayer tous les mots de passe d’un dictionnaire constitué à cet effet.
Voir *Comment sont stockés vos mots de passe*, page 376.

Dictionnaire chiffré

Les dictionnaires chiffrés ou nomenclateurs (ou répertoires) sont des dictionnaires bilingues dont l’une des langues est une langue naturelle comme le français, l’anglais, l’allemand ou le japonais et l’autre une liste de chiffres. Leur gros inconvénient est d’exiger un livre épais, sans être sûr qu’il ne tombera pas aux mains de l’ennemi. Dans ce cas, il n’a plus aucune valeur.
Voir *La saga des dictionnaires chiffrés*, page 39 et *La clef du problème*, page 57.

Digramme

Assemblage de deux lettres consécutives comme DE, EN, IN, etc.
Voir *Chiffrer avec des digrammes*, page 120, fréquence, Playfair.

Elliptique

Voir courbes elliptiques.

Émigrés

Voir *Le chiffre des émigrés*, page 137.

Encodage

Action d’encoder.

Encoder

Verbe plus général que « chiffrer », car on peut encoder dans un but autre que cryptographique. Par exemple, quand un texte est transformé en une suite de bits au moyen du code ASCII, il ne s’agit pas de chiffrement à proprement parler.

Enigma

Machine à chiffrer allemande de la Seconde Guerre mondiale.
Voir *La machine Enigma*, page 292.

Exhaustive

Voir force brute, recherche exhaustive.

Force brute

L’attaque par force brute consiste à tester toutes les clefs possibles d’un algorithme de chiffrement, jusqu’à trouver la bonne. Elle n’est pas efficace pour des clefs de 128 bits ou plus. On parle aussi de recherche exhaustive.

Voir *Faiblesse du DES*, page 353, *Hacher pour sécuriser*, page 372.

Francs-maçons

Voir Pig-Pen.

Fréquence

Pourcentage d'apparition d'une lettre, d'un digramme ou d'un mot dans une langue ou un texte. Calculer les fréquences d'apparition des lettres dans un message est la première étape d'une cryptanalyse.
Voir *L'énigme des Templiers*, page 74, *Les digrammes disent tout*, page 117.

Friedman

William Friedman est l'un des grands noms de la cryptographie.
Voir indice de coïncidence.

Grille de Cardan

Rectangle de carton ou de métal présentant des trous qu'on pose sur une feuille de papier. On l'utilise en écrivant le message dans les trous, avant de retirer la grille et de compléter le texte afin qu'il semble anodin.
Voir *Bas les masques*, page 35.

Grille tournante

Méthode de chiffrement par transposition consistant à écrire à travers une grille, qu'on fait tourner trois fois de 90°.
Voir *Bas les masques*, page 35.

Gripenstierna

Voir machine de Gripenstierna.

Gronsfeld

Chiffrement identique à celui de Vigenère.
Voir Vigenère.

Hachage

Fonction appliquée à un document de longueur variable renvoyant un autre de longueur fixe, caractéristique du document, appelé son résumé ou son haché. Le hachage sert pour stocker les mots de passe ou pour authentifier des documents.
Voir *Hacher pour sécuriser*, page 372.

Henri II

Voir boîte à chiffrer d'Henri II.

Hill

Lester Hill est un mathématicien américain à l'origine d'un chiffre généralisant celui de Playfair.
Voir *Le chiffre de Hill, ou l'irruption des maths*, page 143.

Homophonie

Voir substitution mono-alphabétique.

Homomorphie

Voir chiffrement homomorphe.

Indice de coïncidence

Indice invariable par permutation des lettres. Il permet de reconnaître si un texte, ou une portion de celui-ci, a été chiffré par une substitution mono-alphabétique. Il est utile en cryptanalyse des chiffres poly-alphabétiques Voir *Les coïncidences de Friedman*, page 244, *La position des rotors*, page 307.

Intégrité

Assurer l'intégrité de données consiste à permettre la détection de modifications volontaires faites sur ces données.
Voir authentification.

Jefferson

Voir cylindre.

JN-25

Voir chiffre de la marine japonaise.

Kasiski

La méthode de Kasiski, inventée par Babbage, sert à casser un chiffre de Vigenère.
Voir *La méthode de Kasiski*, page 232.

Kerckhoffs

Grand théoricien de la cryptographie, sans doute le plus grand. Il a énoncé le principe qui porte son nom, toujours d'actualité, selon lequel il vaut mieux qu'un chiffre soit protégé par une clef que par le secret. Il a également donné une méthode de décryptement des chiffres poly-alphabétiques valable quand on dispose d'un grand nombre de messages chiffrés avec la même clef.
Voir *La clef du problème*, page 57, *La méthode de Kerckhoffs*, page 227.

Logarithme discret

Voir *Les courbes elliptiques*, page 366.

Machine de Lorenz

Machine à chiffrer allemande, réservée aux échanges entre le haut quartier général et les armées. Le premier ordinateur (Colossus) a été créé pour décrypter ses messages.
Voir *La machine de Lorenz et Colossus*, page 318.

Machine de Gripenstierna

Cryptographe en forme de cylindre nécessitant deux opérateurs, un côté clair, un autre côté chiffré.
Voir *La machine de Gripenstierna*, page 282.

Machines françaises

Voir B-211, C-36, CX-52, CD-47 et Myosotis.

Masque jetable

Seule méthode de chiffrement dont il a été démontré qu'elle était sûre. Cette démonstration repose cependant sur une hypothèse forte : la clef doit être aléatoire, ce qui n'est pas si facile à assurer. Si la clef est pseudo-aléatoire, le masque jetable est attaquable par la méthode du mot probable.
Voir *Le masque jetable*, page 239.

Méthode de saint Urlo

Méthode consistant à utiliser les dix lettres les plus fréquentes pour détecter une substitution mono-alphabétique. Elle sert à décrypter les chiffrements poly-alphabétiques.
Voir *La méthode de saint Urlo*, page 235.

Mono-alphabétique

Voir substitution mono-alphabétique.

Mot probable

La méthode du mot probable consiste à rechercher un mot que l'on estime probable dans un texte, afin de le décrypter.
Voir *Une affirmation péremptoire*, page 45, *Le mystère du scarabée d'or*, page 84, *Le défi du tueur du zodiaque*, page 134, *Les lettres de Marie-Antoinette*, page 211, *Le mot probable de Jules Verne*, page 221, *Le mot probable de Bazeries*, page 238, *Le décryptement de Turing*, page 309.

Myosotis

Première machine à chiffrer française entièrement électronique.
Voir *La C-36*, page 324.

Napoléon I^er^

Empereur des Français réputé pour la mauvaise qualité de ses chiffres.
Voir *La régression de la Révolution et de l'Empire*, page 154, *la Grande Armée =la Grande Photocopieuse*, page 158.

Nombres

Voir stations de nombres.

Nomenclateur

Synonyme de dictionnaire chiffré.
Voir dictionnaire chiffré.

Objets connectés

Objets connectés à Internet, par nature difficiles à protéger.
Voir *Le danger des objets connectés*, page 378.

PGP

Pretty good privacy. Cryptosystème moderne permettant une bonne confidentialité des échanges.
Voir *Un « niveau de confidentialité correct » : PGP*, page 377.

Pig-Pen

Chiffre à substitution mono-alphabétique utilisé par les francs-maçons.
Voir *L'écriture secrète des francs-maçons*, page 81.

Playfair

Chiffre à substitution digrammique dû à Charles Wheatstone.
Voir *Le chiffre de Playfair*, page 138.

Poly-alphabétique

Voir substitution poly-alphabétique.

Polybe

Général grec, auteur d'un système de transmission qui fut employé ultérieurement comme chiffre.
Voir carré de Polybe.

Porte dérobée

Faille placée volontairement par le concepteur d'un système cryptographique pour donner l'accès au clair d'un message chiffré.

Pourpre

Voir code pourpre.

Probable

Voir mot probable.

Pseudo-aléatoire

Une suite de nombres pseudo-aléatoires est une suite possédant toutes les qualités mathématiques du hasard. Ces suites sont précieuses pour réaliser des simulations de phénomènes aléatoires. En cryptographie, elles n'ont toutefois pas la qualité des véritables suites aléatoires.
Voir *De l'usage des suites pseudo-aléatoires*, page 334.

Quantique

La cryptographie quantique est un protocole informatique destiné à échanger des clefs de manière sécurisée.
Voir *merveilles quantiques*, page 339.

Rail fence

Voir chiffre zigzag.

Recherche exhaustive

Voir force brute.

Réglette de Saint-Cyr

Dispositif constitué de deux réglettes, dont l'une est coulissante pour chiffrer et déchiffrer le chiffre de Vigenère.
Voir *La réglette de Saint-Cyr*, page 274.

Répertoire

Voir dictionnaire chiffré.

Rot13

Méthode de chiffrement consistant à remplacer un caractère par celui qui le suit 13 rangs plus loin dans l'ordre alphabétique. Ainsi, A devient N, mais U devient H car après Z, on compte A. Rot13 est un cas particulier de César.
Voir César.

RSA

Système de chiffrement asymétrique utilisé dans les cartes bancaires et pour la transmission des clefs, en particulier dans le cryptosystème PGP.
Voir *Principes du système RSA*, page 359, asymétrie, PGP.

Saint Cyr

Voir réglette de Saint-Cyr.

Saint Urlo

En français, les lettres les plus fréquentes sont E et celles de SAINT URLO.
Voir méthode de saint Urlo.

Scytale

Système de chiffrement antique, consistant en un bâton autour duquel on entoure une bande de cuir avant d'écrire sur celle-ci.
Voir *La scytale*, page 163.

Shannon

Grand nom de la cryptographie. Il a montré l'inviolabilité sous conditions du masque jetable.

Signature

Donnée courte prouvant l'identité de l'émetteur d'un message.
Voir *Comment sécuriser ses données informatiques*, page 371.

Sigsaly

Machine à chiffrer la voix de la Seconde Guerre mondiale.
Voir *Le chiffrement de la voix*, page 327.

Stations de nombres

Stations de radio n'émettant que des nombres.
Voir *Les stations de nombres*, page 244.

Stéganographie

Procédé consistant à cacher l'existence d'un message, celui-ci pouvant de plus être chiffré.
Voir *L'arme de la guerre secrète*, page 13.

Substitution mono-alphabétique

Le chiffrement par substitution mono-alphabétique consiste à remplacer chaque lettre d'un message par un symbole convenu à l'avance. Ce chiffre est facilement cassable en recourant à la méthode des fréquences. On parle de substitution homophonique si une même lettre peut être remplacée par plusieurs symboles, ce qui permet de rendre la méthode des fréquences plus difficile à appliquer. La méthode du mot probable reste alors une bonne méthode d'analyse.
Voir fréquence, mot probable.

Substitution poly-alphabétique

Une substitution poly-alphabétique consiste à remplacer chaque lettre d'un message par un symbole choisi en fonction de l'état du système. Les plus célèbres

substitutions poly-alphabétiques sont celles de Vigenère (ou de Gronsfeld), du cylindre de Bazeries repris par l'armée américaine sous le nom de M-94 et de la machine allemande Enigma.
Voir *Les substitutions à plusieurs alphabets*, page 201, *Le cylindre de Bazeries*, page 284, *La machine Enigma*, page 292, Vigenère.

Surchiffrement

Fait de chiffrer un message déjà chiffré.
Voir *Le coffre-fort à code secret : surchiffrement*, page 249.

Symétrique

Se dit d'un algorithme de chiffrement utilisant la même clef pour chiffrer et déchiffrer.
Voir *La magie des chiffres asymétriques*, page 357.

Templiers

Voir *L'énigme des Templiers*, page 74.

Tournante

Voir grille tournante.

Transposition

Les chiffres par transposition consistent à permuter les lettres d'un message d'une façon convenue à l'avance.

Voir *Les chiffres par transposition*, page 163.

Trithème

Cryptologue, un des inventeurs des substitutions poly-alphabétiques. Voir *Les litanies de Trithème*, page 32, *Le premier chiffre à mot-clef*, page 202.

Turing

Grand nom de la cryptographie. Il a contribué au décryptement d'Enigma.

Übchi

Chiffre allemand de la Première Guerre mondiale.
Voir *Le système Übchi*, page 180.

Urlo

Voir saint Urlo.

Vernam

Gilbert Vernam est l'inventeur du masque jetable, à l'œuvre en particulier dans le téléphone rouge.
Voir masque jetable.

Vigenère

Blaise de Vigenère est l’un des grands noms de la cryptographie. Chiffrement par substitution poly-alphabétique correspondant à un décalage variable suivant la position de la lettre dans le message donné par une clef.
Voir *Blaise de Vigenère, un personnage multiple*, page 205.

Wadsworth

Voir cadran de Wadsworth.

Zigzag

Voir chiffre zigzag.

BIBLIOGRAPHIE

Après quelques références générales, cette bibliographie est ordonnée par périodes correspondant en gros à l'ordre des chapitres du livre.

Références générales

David Kahn, *The Code-Breakers, The Comprehensive History of Secret Communication from Ancient Times to the Internet*, Scribner, 1996. Ce livre de 1181 pages est une référence jusqu'aux années 1960. Il est partiellement traduit en français en 405 pages : David Kahn, *La Guerre des codes secrets, Des Hiéroglyphes à l'ordinateur*, Interéditions, 1992.
Fletcher Pratt, *Histoire de la cryptographie, les écritures secrètes de l'Antiquité à nos jours*, Payot, 1940.
Simon Singh, *Histoire des codes secrets, de l'Égypte des pharaons à l'ordinateur quantique*, Le Livre de Poche, 2001.
Philippe Guillot, *La Cryptologie*, *l'art des codes secrets*, EDP Sciences, 2013. Livre plus technique, et moins historique, mais accessible avec un bagage mathématique de début de licence.
Hervé Lehning (dir.), *Cryptographie & codes secrets, l'art de cacher*, Hors-série Tangente, n° 26, POLE, 2006.

Hervé Lehning, *L'Univers des codes secrets – De l'Antiquité à Internet*, Ixelles, 2012.
Sébastien-Yves Laurent (dir.), *Le Secret de l'état*, Nouveau Monde, 2015.

Chasse au trésor

Pour ceux qui sont intéressés par les histoires de pirates et les chasses au trésor, en voici un peu plus sur La Buse, son cryptogramme et son trésor.
Charles Bourel de La Roncière, *Le Flibustier mystérieux, histoire d'un trésor caché*, Le Masque, 1934.
Emmanuel Mezino, *Mon Trésor à qui saura le prendre…*, autoédition, 2014. Ce qu'aurait dit La Buse à la foule depuis l'échafaud un instant avant d'être pendu est rapporté de plusieurs façons, comme le montre le titre de ce second livre.

Chiffres de la Renaissance et de l'âge classique

Blaise de Vigenère, *Traicté des chiffres, ou Secrètes manières d'escrire,* Bourbonnois, 1586. Ce livre est en ligne sur Gallica.
Giovani Baptista Della Porta, *De Fustiuis literarum notis, Vulgo de Ziferis, Libri IIII*, Londini, 1591. Livre en latin de l'époque, qu'on peut lire en ligne sur archive.org.
Hervé Lehning, « La boîte à chiffrer d'Henri II », *Bulletin de l'ARCSI*, n° 41, 2014, p. 89-100.
Hervé Lehning, « Strasbourg, témoin de l'évolution de la cryptologie du 16e au 17e siècle », *Revue de la BNU*, n° 13, 2016. Description de la collection de tables de chiffrements et de lettres chiffrées des archives de la ville de Strasbourg, qu'on peut consulter en ligne.

Émile Burgaud et Étienne Bazeries, *Le Masque de fer, révélation de la correspondance chiffrée de Louis XIV*, Firmin-Didot, 1893. Pour le décryptement du Grand Chiffre de Louis XIV.
Paul-Louis-Eugène Valerio, *De la cryptographie, essai sur les méthodes de déchiffrement*, *suivi du Déchiffrement de la correspondance de Henri IV et du Landgrave de Hesse*, L. Baudoin, 1893.
Antoine Casanova, *Le manuscrit de Voynich*, *Bulletin de l'ARCSI*, n° 28, 2000, p. 60-67.
Bengt Beckman, « An early cipher device : Fredrik Gripenstierna's machine », *Cryptologia*, vol. 26, n° 2, 2010, p. 113-123. Pour la description du cylindre de Gripenstierna.

Le déclin napoléonien

Mark Urban, *The Man Who Broke Napoleon's Codes*, Harper Collins, 2001.
Étienne Bazeries, *Les « Chiffres » de Napoléon I^er^ pendant la campagne de 1813*, M. Bourges, 1896.
André Lange et Émile-Arthur Soudart, *Traité de cryptographie*, Félix Alcan, 1925. Ce dernier livre est consultable en ligne sur Gallica.

Le renouveau de la fin du XIX^e^ siècle et du début du XX^e^

Auguste Kerckhoffs, « La cryptographie militaire », *Journal des sciences militaires*, vol. 9, janvier et février 1883, p. 5-38. On trouvera ce document sur le site de l'ARCSI : www.arcsi.fr
Étienne Bazeries, *Les Chiffres secrets dévoilés*, E. Fasquelle, 1901.

Félix Delastelle, *Traité élémentaire de cryptographie*, Gauthier-Villars, 1902. Consultable en ligne sur archive.org.
Gaëtan de Viaris, *L'Art de chiffrer et déchiffrer les dépêches secrètes*, Gauthier-Villars, 1893. Consultable en ligne sur IRIS (université de Lille).
Roger Baudoin, *Éléments de cryptographie*, Pedone, 1939.

Les guerres mondiales et la guerre froide

Louis Ribadeau-Dumas, « Chiffreurs et décrypteurs français de la guerre de 14-18 », *Bulletin de l'ARCSI*, n° 27, 1999, p. 33-53.
Agathe Couderc, « Le Chiffre pendant la Grande Guerre : apprendre à travailler dans l'urgence », *Bulletin de l'ARCSI*, n° 40, 2013, p. 37-48.
Jean-François Bouchaudy, « La machine à chiffrer B-211 », *Bulletin de l'ARCSI*, n° 43, 2016, p. 111-128.
Guy Malbosc et Jean Moulin, *Guerre des codes et guerre navale, 1939-1945*, Marines éditions, 2012.
Philippe Guillot, « Les mathématiciens polonais contre Enigma », *Bulletin de l'ARCSI*, n° 42, 2015, p. 81-94.
Louis Ribadeau-Dumas, « Alan Turing et l'Enigma », *Bulletin de l'ARCSI*, n° 28, 2000, p. 44-52.
Francis Hinsley et Alan Stripp, *Codebreakers : The Inside Story of Bletchley Park*, Oxford University Press, 2001.
David Kahn, *Seizing The Enigma : The Race to Break the German U-Boats Codes, 1939-1943*, Arrow Books, 1996.
Jon D. Paul, « Le système de communication ultra-sécurisé SIGSALY à l'origine de notre monde numérique ? » *Bulletin de l'ARCSI*, n° 44, 2017, p. 69-76.
Olivier Forcade et Sébastien Laurent, *Secrets d'État, Pouvoirs et renseignement dans le monde contemporain*, Armand Colin, 2005. Ce dernier livre est précieux en particulier pour ses chapitres IV et V : un renseignement

désormais incontournable dans les guerres mondiales et le renseignement dans les crises internationales.
Pham Duong Hiêu et Neal Koblitz, « Cryptography During the French and American Wars in Vietnam », *Cryptologia*, vol. 41, n° 6, 2017, p. 491-511.

Époque contemporaine

Jacques Stern, *La Science du secret*, Odile Jacob, 1998.
Pierre Barthélemy, Robert Rolland et Pascal Véron, *Cryptographie : Principes et mises en œuvre*, Lavoisier, 2005.
Douglas R. Stinson, *Cryptography: Theory and Practice*, Chapman & Hall, 2006.
Jean-Paul Delahaye, « Qu'est-ce qu'une blockchain ? », *Bulletin de l'ARCSI*, n° 44, 2017, p. 97-108.
Joël Lebidois, « Cryptomonnaies, consensus distribué et blockchain », *Bulletin de l'ARCSI*, n° 43, 2016, p. 129-136.
Renaud Lifchitz, « Les premiers ordinateurs quantiques accessibles : quels impacts sur la sécurité ? », *Bulletin de l'ARCSI*, n° 42, 2015, p. 115-121.
Chantal Lebrument et Fabien Soyez, *Louis Pouzin, L'un des pères de l'Internet*, Economica, 2018.

CRÉDITS

p.17 : © Mary Evans Picture Library / Photononstop ; p.19 : Collection particulière ; p.20 : © Archives municipales de la ville de Strasbourg ; p.25 : Source : Revue « Miroir de l'Histoire », septembre 1962 – Droits réservés ; p.30 : © Alamy / Photo 12 ; p.41 : Source : Zimmermann Telegram as Received by the German Ambassador to Mexico ; 1/16/1917 ; 862.20212 / 57 through 862.20212 / 311 ; Central Decimal Files, 1910 – 1963 ; General Records of the Department of State, Record Group 59 ; National Archives at College Park, College Park, MD. ; p.43 : © Jon D. Paul, ARCSI ; p.45, 47 : © Musée des Transmisisons – Cesson-Sévigné ; p.51 : © Bundesarchiv, Bild 134-B2501 ; p.54 : © BPK, Berlin, Dist. RMN-Grand Palais / image BPK ; p.55 : © ARCSI ; p.58 : © DeAgostini / Leemage ; p.60 : Collection particulière ; p.71 : Droits réservés ; p.83 : © Archives municipales de la ville de Strasbourg ; p.93 : © Leopold Museum, Vienna, Austria / Bridgeman Images ; p.98 : © Photo by PhotoQuest / Getty Images ; p.110 haut : Source : Extrait de la rubrique correspondances personnelles du 1er janvier 1890 dans Le Figaro ; p.110 bas : Source : La rubrique correspondances personnelles du 12 janvier 1890 dans Le Figaro ; p.112 : Source : La rubrique correspondances personnelles du 23 janvier 1890 dans Le Figaro ; p.113 : Source : La rubrique correspondances personnelles du 20 février 1890 dans Le

Figaro ; p.114 : © Daniel Tant / ARCSI ; p.121, 128 : © Archives municipales de la ville de Strasbourg ; p.130 : Extrait du Bulletin nº1 de l'Association des Réservistes du Chiffre, par Edmond Lerville © ARCSI ; p.131 : © Archives municipales de la ville de Strasbourg ; p.133 : The National Archives, ref. SP53/22 f.1 ; p.135 : © Costa / Leemage ; p.143 : Source : POF-PSF-PT109-1, John F. Kennedy Presidential Library and Museum, Boston ; p.148, 149, 150-151, 152 : © Archives municipales de la ville de Strasbourg ; p.153 : © Archives nationales ; p.181 : Collection particulière ; p.185 : Source : Le Matin, 7 novembre 1914 ; p.199 : Cipher manuscript (Voynich manuscript). General Collection, Beinecke Rare Book and Manuscript Library, Yale University ; p.200 : Cipher manuscript (Voynich manuscript). General Collection, Beinecke Rare Book and Manuscript Library, Yale University ; p.205 : © ARCSI ; p.207 : © Archives Nationales ; p.212 : © Archives nationales ; p.214 : © Archives nationales ; p.216 : Timken Collection, National Gallery of Art, NGA Images ; p.218 : © The American Civil War Museum, Richmond, Virginia ; p.225 : © The Hanoi Police Museum. Photo : Neal Koblitz ; p.226 : © U.S. National Security Agency ; p.231 : Collection particulière ; p.233 : © SSPL / Science Museum / Leemage ; p.240 : © Akg-images / Science Source ; p.342 : © Jerry Proc ; p.243 : Source : Musée de la CIA ; p.245 : © NSA – National Cryptologic Museum ; p.255 : Collection particulière ; p.257 : © Bundesarchiv, Bild 183-R95807 ; p.262 : © ARCSI ; p.256 : © Service historique de la Défense, GR 16 N 1696 ; p.268 : The National Archives, HW 23/1 ; p.279, 280, 281 : Boîte à chiffrer en forme de livre (inv. E.Cl. 1361), Musée national de la Renaissance – château d'Ecouen. Photographie : collection de l'auteur ; p.284 : © NSA – National Cryptologic Museum ; p.285, 189 : © Musée des Transmisisons – Cesson-Sévigné ; p.293 : © Jon D. Paul, ARCSI ; p.294 : © Bundesarchiv, Bild 101I-769-0229-11A ; p.303 : © Alamy / Photo12 ; p.304 : © Image by ART UK. Provided courtesy

National Museums Liverpool ; p.305 : © SCIENCE PHOTO LIBRARY / SPL – Science Photo Library / Biosphoto ; p.311 : © NSA – National Cryptologic Museum ; p.316 : © Everett Historical / Shutterstock ; p.319 : © Shaun Armstrong for Bletchley Park Trust ; p.320 : © Bletchley Park Trust / SSPL / Leemage ; p.323 : © Jon D. Paul, ARCSI ; p.325 haut : Collection de l'auteur ; p.325 bas : Collection de l'auteur ; p.326 : © ARCSI ; p.358 : Collection particulière, droits réservés ; p.360 : © Anita Ponne / Shutterstock ; p.388 : Source : Laura Poitras / Praxis Films -Licence CC BY SA 3.0.

En dépit de nos recherches ; il nous a été impossible d'établir des droits d'auteur dans certains cas. Que ceux que nous n'aurions pas nommés reçoivent nos excuses et se fassent connaître.

Infographies : Laurent Blondel/Corédoc.

TABLE

Préface
1 - L’arme de la guerre secrète
2 - La saga des dictionnaires chiffrés
3 - Les codes des initiés
4 - Les chiffres par substitution
5 - La révolution de Rossignol et la pincée de désordre
6 - Les chiffres par transposition
7 - Cryptologue… jusqu’à la folie
8 - Les substitutions à plusieurs alphabets
9 - Le coffre-fort à code secret : le surchiffrement
10 - Chiffrer avec des instruments artisanaux
11 - Les machines à chiffrer électromécaniques : Enigma et les autres
12 - L’ère numérique et la cryptographie quantique
13 - La magie des chiffres asymétriques
14 - Comment sécuriser ses données informatiques
Conclusion
Remerciements
Ce Qu’il Faut Décrypter : solutions
Glossaire-Index
Bibliographie
Crédits